BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-245

30 MARCH 2009

AIR COMBAT COMMAND
Supplement

12 JANUARY 2010

SHAW AIR FORCE BASE
Supplement

26 MARCH 2012

Operations

ANTITERRORISM (AT)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **http://www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A7S

Certified by: HQ USAF/A7S
(Brig Gen Mary Kay Hertog)

Supersedes: AFI10-245, 21 June 2002

Pages: 117

(ACC)

OPR: HQ ACC/A7SO

Certified by: HQ ACC/A7S
(Colonel Alan R. Metzler)

Supersedes: AFI 10-245_ACCSUP1, 6 May 2003

Pages:21

(SHAWAFB)

OPR: 20 FW/CCFP

Certified by: 20 FW/CCFP
(Mitchell A. Price)

Supersedes: AFI10-245_ACCSUP1_SHAWAFB SUP1, 29 January 2008

Pages:29

This instruction implements AFPD 10-2, *Readiness*; Department of Defense Directive (DODD) 2000.12, *Antiterrorism (AT) Program*; Department of Defense Instruction (DODI) 2000.16, *Antiterrorism (AT) Standards*. It establishes responsibilities and guidance for the Air Force (AF) Antiterrorism (AT) Program and integrates security precautions and defensive measures. This Air Force Instruction (AFI) applies to all military and civilian Air Force personnel, Air Force Reserve Command and Air National Guard units and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims/rims.cfm**. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through the appropriate functional's chain of command.

(ACC) AFI 10-245, 30 Mar 2009, is supplemented as follows: It consolidates the procedures and criteria that support Air Combat Command's (ACC) antiterrorism/force protection program. It applies to all ACC installations as well as associate/tenant units on ACC bases. It applies to all ACC-gained Air Force Reserve Command (AFRC) units when listed in AFRCIND 2. This publication does not apply to the Air National Guard (ANG). Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims**/. Contact supporting records managers as required. Send recommended changes to this supplement via AF Form 847, *Recommendation for Change of Publication*, to HQ ACC/A7SO, 129 Andrews Street, Suite 102, Langley AFB VA 23665-2714.

(SHAWAFB) AFI 10-245, dated 30 March 2009, and AFI 10-245_ACCSUP1, 12 January 2010, are supplemented as follows: This publication implements the Shaw Air Force Base Antiterrorism (AT) Program Standards. It identifies specific unit and individual responsibilities required to implement antiterrorism measures. This supplement applies to all units and personnel assigned to Shaw Air Force Base, whether in tenant, reserve, civilian, guard, or active duty status. This publication requires the collection and/or maintenance of information protected by the Privacy Act of 1974. All squadron AT representatives must implement requirements listed within 90 days of publication. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) AFMAN 33-363, *Management of Records*, and disposed of IAW the Air Force Records Disposition Schedule (RDS) located at **https://my.af.mil/afrims/afrims/afrims/rims.cfm**. Contact supporting records managers as required. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s to 20 FW/CCFP, 517 Lance Ave, Shaw AFB, SC 29152; route through your appropriate functional chain of command.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. It incorporates revisions to DODD 2000.12 and DODI 2000.16 including the requirement for an AT level II certified Antiterrorism Officer; the applicability of AT Standards to non-DoD tenants on DoD property; and updated DoD AT Standards. AF functional roles and responsibilities were added or updated to align with the A-staff construct; and several FPCON measures have been revised or updated, to include measures addressing Biological Select Agents and Toxins (BSAT) and Chemical, Biological, Radiological and Nuclear CBRN). Attachment 2-- References to DOD O-2000.12-H, Attachment 4-- AOR-Specific Training, and Attachment 8-- Antiterrorism Resource Allocation Template were removed and replaced with Attachment 4-- Risk Management and Resourcing processes. The following Report Control Symbol (RCS) requirements were removed: HAF-SFC(AR)0126, Training Reports for Antiterrorism Level I and Level II Training, and HAF-SFC(SA)0125, Status of Antiterrorism Report.

(ACC) This supplement is substantially revised and is updated to align with the revised AFI 10-245. Commanders and antiterrorism officers must completely review this document for new requirements and actions.

(SHAWAFB) This document has been substantially revised and must be completely reviewed. This revision realigns information with the paragraphs it is meant to supplement, exempts the Post Office, SAFE Federal Credit Union and Wachovia bank from the provisions and requirements of the 20 FW Antiterrorism Program. Deletes the requirement to use DD Form 2637 to conduct facility security evaluations and replaces it with a localized form.

Chapter 1

AIR FORCE ANTITERRORISM PROGRAM

1.1. Air Force Antiterrorism Program. This instruction establishes guidance and procedures for the Air Force (AF) Antiterrorism (AT) Program supporting the Department of Defense (DOD) AT Program. The program seeks to deter or limit the effects of terrorist acts against the AF by giving guidance on collecting and disseminating timely threat information, providing training to all AF members, developing comprehensive plans to deter and counter terrorist incidents, allocating funds and personnel and implementing AT measures.

1.1.1. AT Responsibility. AT is a command responsibility and must be thoroughly integrated into every unit mission. Commanders must continually review their AT posture to keep current with changing policies and threat levels. Risk management is the key when determining vulnerabilities and resource prioritization. Any threat or potential vulnerability with risk that cannot be controlled to an acceptable level must be forwarded to the next level in the chain of command for resolution. AT also requires every individual's participation to maintain awareness, practice personal security measures and report suspicious activity.

1.1.2. Countering the Threat. Countering the terrorist threat requires a fully integrated and coordinated AT approach with a number of key areas that include at a minimum: Civil Engineers (Readiness and Emergency Management, Facilities Engineering, Explosive Ordnance Disposal (EOD) and Fire Emergency Services), chemical, biological, radiological, nuclear and high-yield explosives (CBRNE) defense, Services (food), Public Affairs, Communications, Intelligence, Operations, Security Forces, Surgeon General, Judge Advocate, Comptroller and Air Force Office of Special Investigations (AFOSI). AT programs should be coordinated with overarching efforts to achieve protection, such as Force Protection (FP), critical infrastructure protection and continuity of operations, as described in Joint Publication (JP) 3-07.2, *Antiterrorism*.

1.1.2. **(ACC)** Countering the Threat. The Installation Antiterrorism Officer (ATO), as the commander's antiterrorism advisor, is a critical member of the aforementioned group to counter the threat.

1.1.3. DOD Policy. DODD 2000.12, *DOD Antiterrorism (AT) Program*, establishes the DOD policies and responsibilities for the implementation of the DOD AT Program. It establishes DODI 2000.16, *DOD Antiterrorism (AT) Standards*, and DOD O-2000.12-H, *Antiterrorism Handbook*. The DOD AT Program is a sub-element of Combating Terrorism (CbT). Combating Terrorism is a pillar of FP.

1.1.3.1. An active AT program utilizes DOD AT Standards prescribed in DODI 2000.16 as baseline standards. AF AT Standards in Chapter 2 of this document incorporate and supplement the DoD AT Standards and provide AF specific guidance.

1.1.3.1.1. Geographic Combatant Commander AT policy precedence. In accordance with the Unified Command Plan (UCP) and DODD 2000.12, the Geographic Combatant Commander (GCC) AT policies take precedence over the AT policies and programs of any other DOD Component operating or existing in the GCC area of responsibility (AOR) except for those under the security responsibility of a Chief of

Mission (CoM), to include exercising tactical control (TACON) for FP. TACON for FP is in addition to a Combatant Commander's normal exercise of operation control (OPCON) over assigned forces. All DOD personnel traveling into a GCC's AOR shall familiarize themselves and comply with all AOR-specific AT policies. AF Components to GCCs bridge gaps between GCC and AF policies. In the application of AT policy the more restrictive guidance will be applied.

1.1.3.1.1.1. **(Added-SHAWAFB)** The AT program for Shaw Air Force Base will be outlined in two documents. AFI 10-245_SHAWAFB SUP1, *Air Force Antiterrorism Program Standards*, provides guidance on day-to-day operations and responsibilities associated with managing the Antiterrorism program. Shaw AFB OPLAN 10-245, *Installation Antiterrorism Plan,* will cover terrorism threat assessments, terrorist incident response measures and terrorist consequence management measures. 20 FW/CCFP is the overall OPR for both of these documents.

1.1.4. Non-DOD Tenants on AF Property. Commanders shall ensure that there is a host tenant agreement with all non-DOD tenants on AF property and that it specifically obligates the non-DOD tenant to comply with the AT requirements in this AFI. Non-DOD tenants on an AF installation, facility or other AF property will be incorporated into, comply with and support installation security and AT Program requirements. Non-DOD tenants on AF property must comply with all aspects of the AT Program addressed in this Instruction and other AT guidance documents unless the facility is outside of the installation controlled perimeter; DOD personnel occupy less than 25% of the facility's net interior useable area in accordance with Unified Facilities Criteria (UFC) 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*; and the installation commander determines AT compliance is not required for that facility.

1.1.4.1. **(Added-SHAWAFB)** DOD personnel occupy less than 25% of the net interior useable area in accordance with Unified Facilities Criteria (UFC) 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*; of Safe Federal Credit Union, Wachovia Bank and the US Postal Service Center. Therefore, these facilities are not required to comply with 20 FW AT program requirements.

1.1.5. Overseas Travel. All AF military personnel, civilians, dependent family members and contractors when supporting DOD operations in accordance with contract provisions and outside of the United States shall comply with theater, country and special clearance requirements (AFI 24-405, *Department of Defense Foreign Clearance Guide,* and DOD 4500.54-M, *DOD Foreign Clearance Manual*) before traveling outside the continental United States (OCONUS).

1.1.5. **(ACC)** Overseas Travel. Commanders will ensure combatant commander and foreign clearance guide requirements are met, and required country travel briefs have been conducted and documented, when personnel are going on leave outside the continental United States (to include Mexico and Canada). Personnel are encouraged to complete the appropriate country travel briefs (website referenced in Paragraph 2.29.2.) to ensure their safety when travel plans have the possibility of day/short trips into a foreign county.

1.1.6. Eagle Eyes. The Eagle Eyes program is an Air Force AT defensive program created to enhance the collection of threat information by educating members of the Total Force and off-base citizens on the nature of terrorist attack-planning activities. Eagle Eyes is a command responsibility and requires every individual's participation to maintain awareness, practice personal security measures and report suspicious behavior. Every AF installation will establish procedures to receive reports of suspicious behavior or indications of terrorist activity.

1.1.6. **(ACC)** Eagle Eyes. Air Force Office of Special Investigations (AFOSI) will administer the program with assistance from security forces (SF), the ATO, and the Air Combat Command (ACC) Threat Information Fusion Cell (TIFC). The local AFOSI duty agent is the primary point of contact during off-duty hours for Eagle Eyes reporting with the local Base Defense Operations Center and/or Security Forces Control Center serving as backup if the duty agent is unavailable. Eagle Eyes notifications will be disseminated to AFOSI, local security forces squadron (SFS), the installation ATO, and the ACC TIFC (**acc.tifc@langley.af.mil**) to ensure information awareness.

1.2. Roles and Responsibilities.

1.2.1. General. AF commanders or civilian equivalent directors assigned AT responsibility shall establish active AT programs using DOD AT Standards prescribed in DODI 2000.16 as baseline standards to reduce vulnerability to terrorism. AF unique requirements contained in this Instruction supplement DOD AT Standards.

1.2.1.1. Major commands (MAJCOMs), field operating agencies (FOAs), direct reporting units (DRUs), AF Components to the GCC, component-numbered AFs (C-NAFs), numbered AFs (NAFs), wings, installation and self-supported separate facilities and commanders or civilian equivalent directors assigned AT responsibility shall have an AT program tailored to the local mission, conditions, terrorist threat and national security environment.

1.2.1.1.1. **(Added-ACC)** Geographically separated units (GSU) attached to an installation will comply with, and be included in the respective AT plan. Stand-alone GSUs will develop and maintain a viable AT program IAW AFI 10-245 as supplemented.

1.2.1.1.2. **(Added-ACC)** Numbered Air Forces (NAF)/Component-NAFs (C-NAF) shall have an active AT program designed to oversee subordinate installation(s) AT programs.

1.2.1.2. Supplements to this instruction by AF activities, such as MAJCOM or installation supplements, shall identify AT specific operational responsibilities. Responsibilities shall include the scope of AT programs for facilities and operations that do not meet the legal definition of an installation, e.g. recruiting offices, Rapid Engineer Deployable Heavy Operations Repair Squadron (RED HORSE) at Guam and other geographic separated units (GSUs).

1.2.1.3. AF activities and action to combat terrorism shall support the GCC as they exercise overall responsibility for AT within their respective AOR. Ensure such activities and actions comply with applicable status of forces agreements (SOFA) and the *DOD Foreign Clearance Manual*.

1.2.1.4. All commanders have the authority and responsibility to enforce appropriate security measures to ensure the protection of DOD elements and personnel subject to their control while pursuing mission accomplishment and shall ensure the AT awareness and readiness of all DOD elements and personnel assigned or attached.

1.2.1.5. For more effective host nation (HN) support commanders shall, as appropriate:

1.2.1.5.1. Ensure HN and/or civil support agreements for AT mutual support are established and exercised with HN/civil support.

1.2.1.5.2. If required HN/civil support agreements to support AT are not established and implemented, up-channel notification of the situation to MAJCOMs and/or AF Components to GCCs, who shall determine if the GCC has agreements established. If not, document the shortfall and inform the AF/A7S.

1.2.1.5.3. Ensure procedures for information sharing are established and implemented within the commander’s span of control in accordance with GCC or CoM guidance or agreements (SOFA, Mutual Aid Agreement (MAA), etc.) and ensure appropriate personnel under their authority, who are responsible for supporting the classification and declassification of records, receive appropriate training.

1.2.1.5.4. Adopt the following key elements to enhance HN support and ensure this information is in AT policy and training: HN support agreements, resources and benefits provided by the United States, working groups and informal outreach activities, training and exercises with HN officials, threat information sharing and positive human capital attributes of key AF personnel, such as right skills, training and duty tour length.

1.2.1.5.5. For OCONUS permanent or expeditionary assignments, identify qualified interpreters or provide language and cultural training for those personnel filling key positions interacting with HN personnel; consider improving cultural training for all OCONUS permanent party and for pre-deployment.

1.2.2. Financial Management (FM). The FM shall:

1.2.2.1. Advise commanders, the AT Working Group (ATWG) and AT Executive Committee (ATEC) on financial processes and procedures to effectively resource AT program requirements through the planning, programming, budgeting and execution (PPB&E) and Combating Terrorism Readiness Initiative Fund (CbT-RIF) processes in conjunction with other staff offices.

1.2.2.2. Provide long range financial planning for the AT Program.

1.2.3. Inspector General (IG). The Inspector General will evaluate the commander’s ability to execute an AT program and the overall AT program effectiveness will be recorded in accordance with AFI 90-201, *Inspector General Activities*.

1.2.4. Judge Advocate (JA). The JA will provide legal advice on AT matters.

1.2.5. Public Affairs (PA). The PA shall:

1.2.5.1. Incorporate communication activities to combat terrorism in the public affairs program.

1.2.5.1.1. **(Added-SHAWAFB)** Ensure the Shaw Air Force Base community stays informed by using the commander's channel, base bulletin board system (base information system), base marquee and the “Shaw News” base paper for notifications and awareness tips upon implementation of FPCON changes.

1.2.5.1.2. **(Added-SHAWAFB)** Use base information system for continuous reminders of the current FPCONs, as well as publicizing the 20 SFS Crime Stop Lines (x-3669, x-3670) and AFOSI (x-2403) as methods to report suspicious activity.

1.2.5.2. Coordinate all terrorist incident/threat report releases to the media with the commander’s Threat Working Group (TWG) prior to the unit commander’s approval for release.

1.2.5.3. In response to a possible or real terrorist threat, the PA representative, after coordination with the commander’s TWG and the Office of the Assistant Secretary of Defense (OASD)/PA, may acknowledge that increased security measures have been taken. Requests for coverage of counter-terrorism forces will not be approved.

1.2.5.3. **(ACC)** Installation Public Affairs (PA) offices will work closely with the installation ATO ensuring AT/FP articles are periodically incorporated in the base media. Additionally, all articles containing security procedures or photos will be coordinated through the ATO, SFS and wing Operations Security (OPSEC) monitor for approval prior to publication.

1.2.6. Surgeon General (SG). The SG shall:

1.2.6.1. Serve as the OPR for Force Health Protection (FHP) and the Public Health Emergency Officer (PHEO) in accordance with AFI 10-2603, *Emergency Health Powers on Air Force Installations*.

1.2.6.2. Participate in the food and water protection programs as outlined in AFI 10-246, *Food and Water Protection Program*.

1.2.6.3. Ensure food and water vulnerabilities and toxic industrial chemical/toxic industrial material (TIC/TIM) vulnerabilities related to terrorism are entered in the Core Vulnerability Assessment Management Program (CVAMP), through the Antiterrorism Officer (ATO), and are tracked to the commander’s risk acceptance or resolution.

1.2.7. Safety (SE). SE shall assist functional areas in ensuring safety is observed during AT operations and incident management contingencies.

1.2.8. Manpower, Personnel and Services (A1). The A1 shall:

1.2.8.1. Provide AT policy and guidance for personnel issues.

1.2.8.2. Provide specific policy and guidance for documenting pre-deployment AT training and special position or duty qualifications on deployment orders.

1.2.8.3. Ensure a system exists for tracking formal AT training (Standard 24).

1.2.8.4. Serve as the OPR for incorporating and utilizing AT processes concerning food handling and distribution.

1.2.8.5. Assist in the review of Capability Based Manpower Standards and manpower determinant tools for appointed AT positions, e.g. ATOs, as described in AFI 38-201, *Determining Manpower Requirements*.

1.2.8.6. Notify AF/A7S when a deficiency is identified in manpower standards supporting appointed AT positions.

1.2.9. Intelligence, Surveillance and Reconnaissance (A2). The A2 shall provide Intelligence support as directed in AFI 14-119, *Intelligence Support to Force Protection*.

1.2.10. Operations (A3). The A3 shall:

1.2.10.1. Identify AT requirements and desired effects for mission operations.

1.2.10.2. Ensure operational reporting procedures for AT associated events are established and exercised.

1.2.10.3. AF/A3/5 is the OPR for Air Force AT matters and policies and approves all AF-wide AT programs.

1.2.11. Logistics Readiness (A4). The A4 shall:

1.2.11.1. Provide Supply Chain Management to fulfill AT requirements.

1.2.11.2. Monitor logistics readiness AT program support.

1.2.11.3. Manage Airmen support requirements (protective equipment, weapons, etc).

1.2.11.4. Incorporate AT considerations in the expeditionary support planning program.

1.2.12. Operational Plans and Requirements (A5). The A5 shall ensure AT is factored into operational plans, pre-deployment site surveys, airfield, work center, billets and recreation site selections.

1.2.13. Communication (A6 or XC). The A6 or XC shall:

1.2.13.1. Ensure net-centric communications and information (C&I), to include wireless, radio and satellite communications, identifies and links Information Operations capabilities that support AT and provides routine AT communications management and command and control.

1.2.13.2. Assist in the identification of C&I requirements for the AT Program and provide technical solution and rough order of magnitude costings.

1.2.13.3. Ensure C&I vulnerabilities in information systems that support AT Programs are entered into CVAMP, through the ATO, and documented in the system security certification and accreditation package. The vulnerability should be documented as a plan of action and milestone (POA&M) as defined in AFI 33-202, vol 1 *Network and Computer Security*.

1.2.13.4. Provide AT policy and guidance for mail handling and management.

1.2.14. Installation and Mission Support (A7). The A7 shall:

1.2.14.1. Ensure installation capabilities and resources support the AT Program and are incorporated in appropriate aspects of air, space and information operations, plans and requirements.

1.2.14.2. Ensure appropriate capabilities of the AT Program are integrated with the Emergency Management (EM) Program as defined in AF Policy Directive (AFPD) 10-25, *Emergency Management*, and AFI 10-2501*, Air Force Emergency Management (EM) Program, Planning and Operations*.

1.2.14.3. Implement terrorism incident planning for response, consequence management and recovery within AT Programs.

1.2.14.4. Provide engineering infrastructure protection expertise to counter terrorist threats.

1.2.14.5. Ensure installation programmers and engineers are trained in FP and AT and incorporating the latest DOD and UFC standards in all designs.

1.2.14.6. Contracting officers, in coordination with program managers and requirement officials, ensure AT clauses required by Defense Federal Acquisition Regulation (DFAR) and supplements and local AT measures provided as part of the requirement are incorporated into AF contracts (Standard 18).

1.2.14.7. Provide physical security and provost service capabilities to support AT.

1.2.14.8. Ensure appropriate capabilities of the AT Program are integrated with Integrated Defense as defined in AFPD 31-1, *Integrated Defense.*

1.2.14.9. Ensure engineering infrastructure, installation and/or facility design, physical security, resource protection, fire emergency services, EOD, expeditionary engineering, and readiness and emergency management vulnerabilities related to terrorism are entered in CVAMP, through the ATO, and the Automated Civil Engineering System (ACES).

1.2.14.9.1. **(Added-ACC)** Civil Engineer (CE) Programmers, with the aid of the installation ATO, will ensure Core Vulnerability Assessment Management Program (CVAMP) tracking numbers are input in the “VAMP Reference” block and ATF is selected as the Programming Sub Source (if applicable) for Automated Civil Engineering System (ACES) loaded projects.

1.2.14.9.2. **(Added-ACC)** Installations must ensure sustainment and/or preventative maintenance costs for AT/FP security requirements are incorporated.

1.2.14.10. AF/A7S drafts and coordinates AF-wide AT matters, policies and programs.

1.2.15. Strategic Plans and Programs (A8). The A8 shall:

1.2.15.1. Provide long-term planning and programming for AT programs and processes.

1.2.15.2. Develop, integrate and analyze AT initiatives for AF Future Years Defense Program (FYDP) and long range plan to support the National Military Strategy for Combating Terrorism.

1.2.15.3. Ensure AT programming initiatives are considered for operational impact during PPB&E processes.

1.2.16. Air Force Office of Special Investigations (AFOSI). Provides the Air Force a capability to conduct Counterthreat Operations (CTO) to detect and assess – *find, fix, track and neutralize* the enemy threat as described in AF Tactics, Techniques, and Procedures (AFTTP) 3-10.3, *Integrated Defense Counterthreat Operations (CTO).* AFOSI is the lead

Air Force agency for collection, investigation, analysis and response for threats arising from terrorists, criminal activity and foreign intelligence and security services as described in AFPD 71-1, *Criminal Investigations and Counterintelligence* and AFI 14-119, *Intelligence Support to Force Protection (FP).*

1.2.16.1. Provides personal protective services for High-Risk Personnel (HRP) based on threats and in accordance with DODI O-2000.22, *Designation and Physical Protection of DOD High Risk Personnel* and AFI 71-101, vol 2, *Protective Service Matters.*

1.2.17. Antiterrorism Officers (ATOs). The ATO is the commander's military or civilian advisor charged with managing the AT Program. Responsibilities are outlined in Standard 9.

1.2.18. Unit AT Representative. Unit AT representatives are appointed in writing for units and DOD elements and personnel not required to have an ATO as stipulated in Standard 9. Unit AT representatives are charged with managing the AT Program for their unit or DOD element and personnel. Responsibilities are further described in paragraph 2.9.5.

1.2.18.1. **(Added-ACC)** All organizations/units on ACC installations not requiring a Level II-trained ATO IAW Standard 9, [to include tenants (major commands (MAJCOM), Defense Commissary Agency, Department of Defense Education Activity, Army and Air Force Exchange Service, etc) and other DOD agencies], must appoint a primary and alternate unit AT representative (E-5 or above) or civilian equivalent in writing. Once designated, forward a copy of the appointment letter to the installation ATO.

1.2.18.1. **(SHAWAFB)** Utilize the ATO appointment memorandum template in Attachment 7 to develop ATO appointment memos.

1.2.18.2. **(Added-ACC)** Tenant units who do not have military personnel assigned will appoint a civilian primary and alternate AT representative in writing. Once designated, forward a copy of the appointment letter to the installation ATO.

1.2.19. **(Added-SHAWAFB)** Group commanders will appoint one of their supporting staff members as a group ATO to consolidate unit antiterrorism issues and represent the group during Antiterrorism Working Group (ATWG) meetings.

1.2.20. **(Added-SHAWAFB)** Group Antiterrorism Officers will:

1.2.20.1. **(Added-SHAWAFB)** Distribute monthly schedule for Random Antiterrorism Measures (RAMs)

1.2.20.2. **(Added-SHAWAFB)** Coordinate, monitor, track and report antiterrorism taskings within the group to 20 FW/CCFP.

1.2.20.3. **(Added-SHAWAFB)** 20 FW unit commanders and tenant organizations will:

1.2.20.4. **(Added-SHAWAFB)** Appoint a primary and alternate unit AT Officer (UATO) (E-5 or higher, or civilian equivalent) to act as a liaison with the group ATO and 20 FW/CCFP on antiterrorism matters. Units will forward a copy of their UATO appointment memorandum to their respective group ATO and the 20 FW/CCFP. Memoranda of appointment will include all AT courses attended, NIPRNET and SIPRNET email addresses, cell phone or pager number, duty phone information and facilities (by building number) under the responsibility of the appointed individuals. Memoranda of appointment will be updated annually or as changes occur.

1.2.20.5. **(Added-SHAWAFB)** Upon notification by 20 FW/CC or designee, implement the appropriate FPCON actions, as outlined in 20 FW OPLAN 10-245, *Installation Antiterrorism Plan*.

1.2.20.6. **(Added-SHAWAFB)** Publish a unit Operating Instruction (OI) for the AT program. As a minimum, the OI must include established pre-incident requirements outlined in Attachment 8.

1.2.20.7. **(Added-SHAWAFB)** Ensure a Physical Security Evaluations for each facility are conducted/reviewed annually and documented utilizing the checklist in Attachment 9.

1.2.20.8. **(Added-SHAWAFB)** Ensure Level I AT Awareness training is included in the Unit Master Training Plan.

1.2.20.9. **(Added-SHAWAFB)** Provide Antiterrorism training statistics as requested by the 20 FW/CCFP as requested.

1.2.20.10. **(Added-SHAWAFB)** Ensure monthly Random Antiterrorism Measure (RAM) performance reports are filed with the group and 20 FW/CCFP.

1.2.21. **(Added-SHAWAFB)** Unit facility managers will:

1.2.21.1. **(Added-SHAWAFB)** Post FPCON signs on necessary facility entrances as outlined in the unit AT OI.

1.2.21.2. **(Added-SHAWAFB)** Ensure unit facilities comply with all directed FPCON antiterrorism measures and provide feedback to UATOs on the effectiveness or impact of the measures.

Chapter 2

ANTITERRORISM STANDARDS

2.1. Standard 1: AT Program Elements. The minimum required elements of an AT program shall be: risk management (Standard 3); planning (including development of the AT Plan) (Standard 7); training and exercises (Standard 23); resource application (Standard 30); and comprehensive program review (Standard 31). The development and maintenance of the AT Program elements should be ongoing and continuously refined to ensure the relevance and viability of all measures employed to reduce vulnerabilities to terrorist capabilities.

2.2. Standard 2: Intelligence Support to the AT Program.

2.2.1. The Defense Intelligence Agency (DIA) sets the DOD Terrorism Threat Level (TTL). This threat level identifies the potential threat to DOD interests in a particular country, including the United States. The DOD TTL applies whether or not U.S. personnel are present in the country. GCCs may also set terrorism threat levels for specific personnel, family members, units, installations or geographic regions in countries within the GCC AOR. See Attachment 3 for more information on TTLs.

2.2.2. Commanders of MAJCOMs, AF Components to the GCC, C-NAFs, NAFs, wings, installations or self-supported separate facilities or deployed commanders assigned AT responsibility shall:

2.2.2.1. Task the appropriate officials under their command or control to gather, analyze and circulate appropriate terrorism threat information. When local information indicates gaps, commanders shall forward timely requests for information via appropriate intelligence collection and production channels.

2.2.2.2. Identify Intelligence (A2) as the lead force protection intelligence (FPI) representative to develop Priority Intelligence Requirements (PIRs) for integration into the Commander's Critical Information Requirements (CCIRs) to focus collection and analysis efforts.

2.2.2.2.1. The AFOSI has the lead for continental United States (CONUS) related PIRs.

2.2.2.3. Provide units in transit with tailored terrorist threat information.

2.2.2.4. Integrate countersurveillance, surveillance detection, counterintelligence (CI) and other specialized skills into AT programs.

2.2.2.5. Identify an AFOSI official as the focal point for local or host-nation law enforcement intelligence, CI and criminal intelligence (CRIMINT) information.

2.2.2.5.1. **(Added-ACC)** Commander, or Special Agent in Charge (SAIC) Air Force Office of Special Investigations (AFOSI) detachments or their designated representative will be the primary focal point. Installation ATO and SFS will provide assistance if required.

2.2.2.5.2. **(Added-ACC)** AFOSI will provide all relevant threat information affecting the installation, the base populace, or the DOD in general to the installation

ATO & SFS commander, to ensure the installation risk management process has the most up-to-date information. Additionally, the threat working group (TWG) should ensure members have a complete understanding of any/all threats when appropriate.

2.2.2.6. Incorporate proactive techniques to detect and deter terrorists, particularly in support of assets or activities conducted in areas designated with SIGNIFICANT or HIGH TTLs. These activities shall include, but are not limited to: in-transit forces, HRP, special events and high-value military cargo shipments.

2.2.2.7. Ensure that subordinate commanders at all levels forward up and down the chain of command all information pertaining to suspected terrorist threats or acts of terrorism involving DOD elements and personnel or assets for which they have responsibility, including the provisions of such information to appropriate interagency officials.

2.2.2.8. Ensure subordinate commanders and key staff members are trained to maximize the use of information derived from law enforcement liaison from intelligence and CI processes and procedures. This includes intelligence procedures for handling PIR for in-transit units and the implementation of procedures to conduct intelligence preparation of the battle space and mission analysis.

2.2.3. Air Force intelligence, CI and law enforcement elements will coordinate the dissemination of information on U.S. persons to the Air Force as appropriate in support of the AT Program and within the provisions of AFPD 71-1, *Criminal Investigations and Counterintelligence*, AFI 71-101, Vol 1, *Criminal Investigations,* and DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*.

2.2.3.1. **(Added-ACC)** The ACC TIFC will serve as the focal point for the collection, assessment and analysis of all-source threat information pertaining to ACC personnel and resources. Intelligence derived from ACC TIFC analysis will be forwarded up the chain of command to the ACC TWG (actionable intelligence) and/or down the chain of command to subordinate units (situational awareness). To ensure timely identification of potential threats, the three core positions within the ACC TIFC will be staffed by representatives of AFOSI 2nd Field Investigations Region (2 FIR), the ACC Homeland Defense Branch (HQ ACC/A3OH) and the 15th Intelligence Squadron (15 IS).

2.2.3.2. **(Added-ACC)** Intelligence support to force protection IAW AFI 14-119 *Intelligence Support to Force Protection (FP)*, will be incorporated to support the installation AT program.

2.3. Standard 3: AT Risk Management.

2.3.1. The AT risk management process is modeled upon the principles described in DOD O-2000.12-H and Integrated Defense Risk Management described in AFPD 31-1. It should be applied in all aspects of AT program implementation and planning, including operational plans and decisions, development of risk mitigation measures and the prioritization and allocation of resources. The essential components of AT risk management include: determining the criticality of assets (criticality assessment); assessing the terrorist threats (threat assessment); identifying the vulnerabilities of facilities, programs and systems to an attack, including the use of CBRNE or similar capabilities (vulnerability assessment); assessing risk based on a holistic understanding of the criticality, threat and vulnerability of the asset (risk assessment); and implementing the capabilities needed to correct or mitigate the risk (countermeasures) and reevaluating risk after countermeasures are employed; and/or accepting risk.

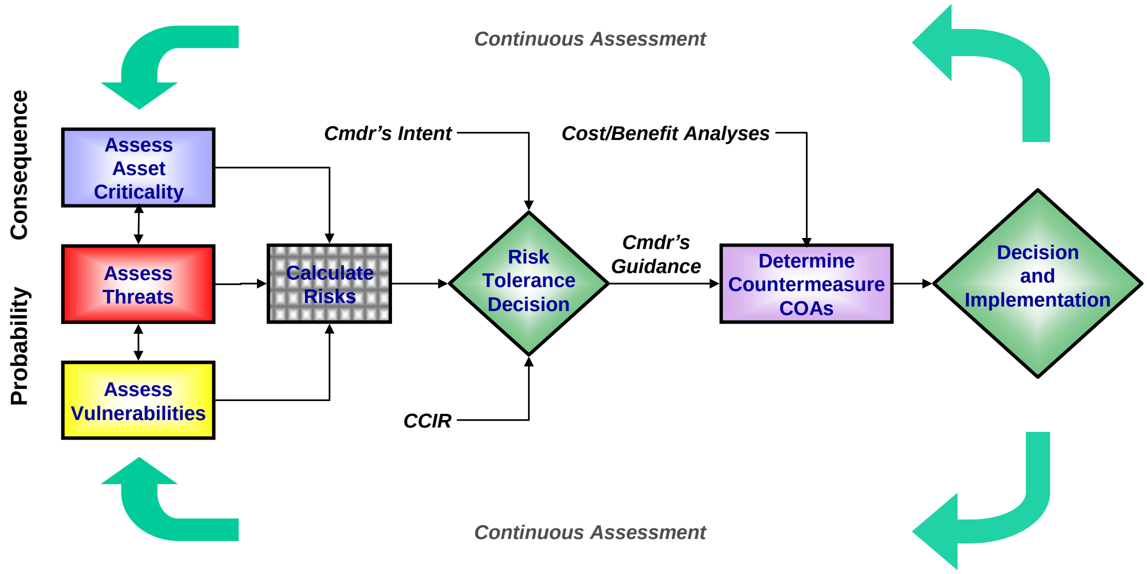
2.3.1.1. The AT risk management process and procedures shall be reviewed at least annually. An AT Program Review, a Higher Headquarters Assessment (HHA) or a Joint Staff Integrated Vulnerability Assessment (JSIVA) visit satisfies this requirement.

2.3.1.1.1. **(Added-ACC)** All subject matter experts (SME) included in the AT risk management process will provide data to the installation ATO for inclusion in the AT plan.

2.3.1.1.2. **(Added-ACC)** Wings should ensure all risk management efforts have been coordinated between all affected agencies/programs (e.g. control assessment risk management, continuity of operations, emergency management) to the maximum extent possible.

2.3.1.2. AT risk management is a continuous process of conducting operations. See Figure 2.1 for a graphical depiction.

Figure 2.1. AT Risk Management Process.



2.3.1.3. For deployments, AT risk management begins with the warning order.

2.4. Standard 4: Terrorism Threat Assessment.

2.4.1. Through the AFOSI and with support from the A2 and ATO a threat assessment process shall be established consistent with the principles outlined in DOD O-2000.12-H to identify the full range of known or estimated threat capabilities (including the use or threat of use of CBRNE). These assessments shall be updated on an annual basis or more frequently as the threat environment dictates or whenever the DIA or GCC TTL changes. Assessments shall be tailored to local conditions. For each group that may be a threat the assessment shall provide information on the group's intent, tactics, techniques and procedures (TTP), capability, probable course of action (COA) and history, as well as any specific targeting information that may be available. AFOSI is the AF agency responsible for preparing the

DOD Threat Assessment (DTA) as prescribed in DODI 5240.18, *Counterintelligence Analysis and Production*.

2.4.2. Specific threat assessments are also prepared to support operational planning and risk decisions for unique mission requirements or special events including, but not limited to, in transit forces, training and exercises, and operational deployments.

2.4.2.1. **(Added-ACC)** AFOSI detachments will conduct localized threat assessments for all large media events, such as open houses, air shows, etc. All threat assessments and counterintelligence special products will be posted on the AFOSI secret Internet protocol router network (SIPRNET) webpage after AFOSI 2 FIR staff validation and HQ AFOSI approval. This webpage will be made available to the installation ATO, SFS Intelligence Flight (SFS/S2), and installation intelligence squadron. However, the detachment will provide a portable document format (.pdf) version of the validated product to these units upon request.

2.4.2.2. **(Added-ACC)** AFOSI will provide a copy of all terrorism threat assessments to the installation ATO for inclusion in the AT plan.

2.4.3. Effective processes should be implemented to integrate and fuse all sources of available threat information from local, State, Federal and host-nation law enforcement agencies; the appropriate local, State, Federal and host-nation intelligence community activities; other local community officials and individuals; the applicable U.S. country team; port authority officials and husbanding contractors, as appropriate, to provide for a continuous analysis of threat information to support the threat warning process in accordance with Standard 2.

2.4.4. Threat assessments are integrated into the AT risk management process as a major source of analysis and justification for recommendations and implementation of Random Antiterrorism Measures (RAMs); AT enhancements including physical security, emergency management or FHP changes; program and budget requests; and when conducting AT vulnerability assessments (VAs).

2.5. Standard 5: Criticality Assessment.

2.5.1. Criticality assessment processes shall be established consistent with the principles described in DOD O-2000.12-H and AFPD 31-1 to identify, classify and prioritize mission-essential personnel, assets and information. Criticality assessments shall also be conducted for non-mission essential assets such as high-occupancy buildings, mass gathering activities, energy infrastructure and any other facility, equipment, service or resource deemed important by the commander warranting protective measures to ensure continued efficient operation; protection from disruption, degradation or destruction; and timely restoration.

2.5.1.1. Criticality assessments should be coordinated with affected Defense Critical Infrastructure Program (DCIP) and Air Force Critical Infrastructure Programs (AF CIP), which follow the principles in DODD 3020.40, *Defense Critical Infrastructure Program (DCIP)*, and AFPD 10-24, *Air Force Critical Infrastructure Program,* and identify defense critical infrastructure and critical assets.

2.5.2. Criticality assessments will be updated at least annually to determine the degree of asset criticality based upon the following factors: relative importance, effect of loss, recoverability, mission functionality, substitutability and repairability. Criticality assessments shall provide the basis for identifying those assets that require specific protective measures and priorities for resource allocation when developing and updating AT-related contingency plans, e.g., AT Plan, Comprehensive Emergency Management Plan (CEMP) 10-2, Medical Contingency Response Plan (MCRP), Integrated Defense Plan (IDP), etc.

2.6. Standard 6: Terrorism Vulnerability Assessment.

2.6.1. Vulnerability assessment processes shall be established consistent with the principles described in DOD O-2000.12-H and AFPD 31-1 to provide a vulnerability-based analysis of personnel (mission essential, mass gatherings, etc.) and mission essential assets (energy infrastructure, etc.) and information that are susceptible to terrorist threats. Incorporate food and water vulnerabilities according to the guidance in AFI 10-246. Incorporate other assessments, such assessments made through the DCIP and AF CIP, or coordinate schedules so teams visit the installation during the same time frame to reduce the impact on operational units.

2.6.1.1. AF VA benchmarks provided by the AF Vulnerability Assessment Team (AFVAT), which include the JSIVA benchmarks, will be used. Within 90 days of a completed assessment, prioritize identified vulnerabilities, develop a plan of action to mitigate or eliminate the vulnerabilities and/or assume risk and report assessment results to the first general officer, flag officer or civilian equivalent director in the chain of command, to include the NAF.

2.6.1.1. **(ACC)** Installation commanders shall address, mitigate and correct AT/FP vulnerabilities identified during all vulnerability assessments, especially procedural or relatively inexpensive and would improve the AT/FP posture. Conversely, high cost improvements must be considered in context with threat and risk assessment, and if necessary, planned for and programmed.

2.6.1.2. CVAMP shall be populated with assessment results, vulnerabilities as a minimum, within 120 days from completion of the assessment, i.e. assessment outbrief.

2.6.1.2.1. **(Added-ACC)** Installations will populate CVAMP within 30 days of receiving the higher headquarters (HHQ) vulnerability assessment (VA) out brief or completing a local assessment. NOTE: The VA out-brief may be used initially to begin analysis/mitigation process, but CVAMP shall be fully populated upon receipt of the final report.

2.6.1.2.2. **(Added-ACC)** Data entry into CVAMP may initially be loaded as “Procedural,” in order to timely input data into CVAMP. Strict follow-up must be maintained to ensure the appropriate installation-level review (TWG and/or ATWG) is conducted to address the vulnerabilities initially entered as “Procedural.” A change to “Programmatic” (if required), project numbers, and funding information must be entered as soon as possible, following installation review.

2.6.1.2.3. **(Added-ACC)** Programmatic vulnerability/concern observations and their respective unfunded requests (UFR) shall be “released” to NAF/HHQ within 120 calendar days of receiving the final report to gain HHQ visibility, and possible funding opportunities. Programmatic observations not able to be populated with funding request data and released to HHQ within 120 calendar days will have corrective action status updated with the limiting factors and estimated date of completion. Use Paragraph 2.6.1.2.6 of this supplement as a guide. NOTE: Incomplete UFRs will be returned to the unit and not be considered for funding.

2.6.1.2.4. **(Added-ACC)** NAF/HHQ shall take action (release or return) appropriate observations/UFRs within 30 days of installation submittal.

2.6.1.2.5. **(Added-ACC)** All procedural observations will be mitigated and closed in CVAMP within 120 calendar days of a completed assessment. Procedural observations not able to be closed within 120 calendar days will have corrective action status updated with the limiting factors and estimated date of completion. Use Para 2.6.1.2.6 of this supplement as a guide.

2.6.1.2.6. **(Added-ACC)** CVAMP data shall be completely reviewed and updated within the first ten (10) workdays of each calendar year quarter (Jan, Apr, Jul, Oct), as a minimum. Annotate and update CVAMP data corrective action status for open observations by performing the following actions.

2.6.1.2.6.1. **(Added-ACC)** Each open observation corrective action status shall be updated using the “Corrective Action Information” option within the observation.

2.6.1.2.6.2. **(Added-ACC)** Within the “Corrective Action Information” screen select the “Review/Edit” button. Update/review all the data associated with the observation corrective action. Select appropriate “Status Update/Action Taken to Close This Observation” category, and add a comment to the action taken. Use the “Status Update” category when updating the status and not closing the observation. Don’t forget to select the “Add” button after entering comments and then the “Validate & Save” button before closing the observation window.

2.6.1.2.6.3. **(Added-ACC)** Corrective Action comments shall include the reason for the observation to remain open, limiting factors for incomplete funding request data, and estimated completion date (if applicable).

2.6.1.2.7. **(Added-ACC)** Installation commanders may authorize installation ATO's "Commanders Privileges" within CVAMP to aid in the database upkeep. However, this does not relieve the commander from having situational awareness of the data. Authorization will be included on the ATO appointment letter.

2.6.1.2.8. **(Added-ACC)** The ACC Security Forces Division (HQ ACC/A7S) shall report CVAMP Vulnerability/Concern/UFR status and command observation trend analysis on a semi-annual basis, as a minimum.

2.6.1.3. A VA will be conducted at least annually or more frequently if the VA or mission requirements dictate. The VA will be conducted by a HHA team at least triennially. VAs shall be conducted at a minimum for, but not limited to:

2.6.1.3.1. Any AF installation or AF owned or leased facility populated daily by 300 or more DOD personnel.

2.6.1.3.2. Any AF installation or facility thereon bearing C2 responsibility for emergency response or physical security plans and programs, or determined to host defense critical infrastructure or critical assets identified through the DCIP or AF CIP, or use, possess, transfer, or receive biological select agents and toxins (BSAT).

2.6.1.3.3. Any AF installation or AF owned or leased facility or activity possessing authority to interact with local non-military or host-nation agencies or having agreements with other agencies or host-nation agencies to procure these services.

2.6.1.3.4. AF hosted air ports of embarkation (POE) and debarkation (POD); movement routes (air, ground and rail); and assembly, staging, reception and final bed down locations in support of any battalion, squadron, ship, or equivalent operational deployment; and similar sized in-transit movement or training exercise. AF movement or shipment of military cargo shall be coordinated with the designated senior DOD Component with AT responsibility.

2.6.1.3.5. Any AF personnel designated as HRP (Standard 16). These assessments are referred to as Personal Security Vulnerability Assessments (PSVAs). PSVAs will conform to the formats of servicing Protection Providing Organizations (PPO) as identified in DODI O-2000.22. AFOSI is a designated PPO.

2.6.1.3.6. Any AF event or activity determined to be a special event or activity involving a gathering of 300 or more DOD personnel.

2.6.1.3.7. AF owned or leased off-installation housing, schools, daycare centers, commissaries, transportation systems and routes used by DOD personnel and their dependent family members when the TTL is SIGNIFICANT or higher, consistent with Standard 3. At locations where there are multiple DOD components or locations that are not AF owned or leased, VA requirements shall be coordinated with the designated senior DOD Component with AT responsibility.

2.6.1.4. Information derived from AT VAs shall be classified pursuant to the requirements outlined in the *Defense Threat Reduction Agency (DTRA)Joint Staff Integrated Vulnerability (JSIVA) Security Classification Guide*.

2.6.2. MAJCOMs and AF Components to the GCC will support the GCCs in scheduling assessments and prescribing policies for no-notice or short-notice movements to locations where a VA has not been accomplished or is not current. MAJCOMs should receive copies of reports on all VAs completed based on Standard 6.

2.6.2. **(ACC)** Forward VA brief and report to the ACC Security Forces Operations Branch (HQ ACC/A7SOA) (SIPR or hard copy) within 10 days of receiving the product(s). Maintain reports in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims**/.

2.6.3. **(Added-SHAWAFB)** Collection and recording of vulnerabilities:

2.6.3.1. **(Added-SHAWAFB)** All identified vulnerabilities from local or higher headquarters assessments will be collectively recorded onto a master list and assigned a priority based on the level of risk it exposes the wing's resources to. This master listing will be maintained by the 20FW/CCFP.

2.6.3.2. **(Added-SHAWAFB)** All vulnerabilities will be assigned an OPR and OCRs, if applicable. OPRs will be responsible for providing recurring updates to the 20 FW/CCFP and taking corrective actions to eliminate or mitigate the vulnerability.

2.6.3.3. **(Added-SHAWAFB)** 20 FW/CCFP will ensure the risk/vulnerability assessment is conducted, reviewed and updated as needed. Information related to the vulnerabilities will not be released outside USAF channels without the approval of the wing commander. Certain assessments and reports may not be released without prior approval of the wing commander. Vulnerability information will be disseminated to the Force Protection Executive Council (FPEC) and to the Force Protection Working Group to ensure commanders are aware of the local vulnerabilities when planning for, or adopting, a course of action in view of a particular threat or contingency. Vulnerability assessments will be maintained by the 20 FW/CCFP.

2.7. Standard 7: AT Plan.

2.7.1. Commanders will develop and maintain a comprehensive AT plan for all DOD elements and personnel that the AF has AT responsibility. Use of the Joint Antiterrorism (JAT) Guide, when used in its entirety, satisfies all minimum planning elements prescribed in this instruction. These AT plans will not be considered complete unless signed by the commander and exercised. If applicable, synchronize the AT Plan with any existing CEMP and IDP. At a minimum, AT plans shall be developed at the installation and separate or leased facility or space levels and for AF operational deployments, training exercises or events, and special events.

2.7.1. **(SHAWAFB)** The 20 FW/CCFP is the overall OPR for the installation AT Plan.

2.7.1.1. **(Added-ACC)** Installation commanders will document a review of the Installation AT Plan on an annual basis and within 60 calendar days of assuming command. Installation ATO must maintain the commander's review with the AT Plan. ATO's will maintain a 2-year history of AT plan reviews.

2.7.1.2. **(Added-ACC)** Installation AT plans must be comprehensive, executable and cross-referencing to/with other plans. It can be an annex to the local installation defense plan/integrated defense plan (typically local OPLAN 31) to ensure a truly integrated defense plan and avoid conflicting requirements across multiple plans. This annex/plan can also serve as the installation supplement to this instruction. An example of a plan is provided in Attachment 6 of this supplement. The AT plan should integrate all base and community actions to deter, detect, defend, and respond to terrorist actions. Relevant portions of existing plans may be annexed into the installation AT plan.

2.7.1.3. **(Added-ACC)** Each unit (e.g. detachment, squadron, group/wing staff, MAJCOM directorate, etc.) will create a checklist with specific unit measures designed to support the base AT program, including random and force protection condition implementation. The installation ATO will maintain/file appropriate checklists.

2.7.2. AT principles are incorporated into all operational plans and risk decisions using the standards prescribed by this instruction as a baseline to develop and implement AT policies in support of the AF's unique roles and mission requirements. Table 2.1. incorporates the Homeland Security Presidential Directive (HSPD) 8, *National Preparedness*. The OPR will recommend the appropriate planning parameters regarding the scale for AF operations and civil support operations based on the threat. Where A7C (CE) is designated the OPR, refer to AFI 10-2501.

Table 2.1. AT Threat Planning Scenarios.

Scenario	Title	OPR
1	Nuclear Detonation – 10-Kiloton Improvised Nuclear Device	A7C (CE)
2	Biological Attack – Aerosol Anthrax	A7C (CE)
4	Biological Attack – Plague	A7C (CE)
5	Chemical Attack – Blister Agent	A7C (CE)
6	Chemical Attack – Toxic Industrial Chemicals	A7C (CE)
7	Chemical Attack – Nerve Agent	A7C (CE)
8	Chemical Attack – Chlorine Tank Explosion	A7C (CE)
11	Radiological Attack – Radiological Dispersal Devices	A7C (CE)
12	Explosive Attack – Bombing Using Improvised Explosive Devices	A7C (CE)
13	Biological Attack – Food Contamination	SG3 (Medical)
15	Cyber Attack	XC or A6
16 (AF)	Armed Attack – Small Arms: Individual to Squad (10 pax)	A7S (SF)
17 (AF)	Aircraft Attacks in the Take-off and Landing Footprint	A7S (SF)
18 (AF)	Stand-off Indirect Fire	A7C (CE)
19 (AF)	Sniper Attack	A7S (SF)
20 (AF)	Hostage Crisis	A7S (SF)
21 (AF)	Contamination of Drinking Water System	SG3 (Medical)
22 (AF)	Extended Loss of Energy Supply	A7C (CE)
Note: Scenarios are numbered to correspond to the national scenarios, except for AF added scenarios		

2.7.3. Tailor AT plans to the level of command or activity for which the AT principles were developed. AT plans may reference information from installation contingency response plans. At a minimum AT plans shall address:

2.7.3.1. The minimum essential AT program elements (AT Standard 1) and standards prescribed by this instruction.

2.7.3.2. Specify risk correction or mitigation measures to establish a local baseline defensive posture. The local baseline defensive posture shall facilitate systematic movement to and from elevated security postures, including the application of RAMs.

2.7.3.3. AT physical security measures (Standard 13).

2.7.3.4. AT risk mitigation measures for AF off-installation facilities, housing and activities (Standard 15).

2.7.3.5. AT risk mitigation measures for HRP (Standard 16).

2.7.3.6. AT construction and building considerations (Standard 17).

2.7.3.7. AT risk mitigation measures for logistics and other contracting (Standard 18).

2.7.3.8. AT risk mitigation measures for critical asset security (Standard 19).

2.7.3.9. AT risk mitigation measures for in-transit movements.

2.7.3.10. AT incident response measures (Standard 20).

2.7.3.11. Terrorism consequence management measures, including CBRNE and weapons of mass destruction (WMD) mitigation planning (Standard 21 and CEMP 10-2).

2.7.3.12. FPCON implementation measures, including site-specific AT measures (Standard 22).

2.7.4. GCCs provide AT planning information (e.g., airfield, port and movement route information and criticality, threat and VA data) to deploying DOD units; and, directs the execution of advance site reviews to facilitate the AT planning process in areas where the assessed TTL is SIGNIFICANT or HIGH or where a specific Terrorism Warning is in effect.

2.7.4.1. At the discretion of the GCC, such security efforts may be waived for deployments or visits to controlled locations such as existing military installations. Augmentation of assessment personnel may be necessary to enable subordinate AF Component commanders to discharge their responsibility to provide security, surveys, assessments, CI and countersurveillance support, and to act as the liaison with the country team, host-nation security force, contractors and port authority.

2.7.5. In countries where available, AFOSI special agents are assigned to FP Detachments (FPD) and provide FP and CI services to in-transit DOD personnel. FPDs are mandated to provide surveys, assessments, CI and countersurveillance support, and act as the liaison with the country team, host-nation security forces, contractors and port authority.

2.7.6. Coordinate AFOSI support for large exercises, contingencies and special events in foreign countries.

2.7.7. Ensure plans include procedures to expedite off-base first and emergency responders onto the installation during increased FPCON.

2.8. Standard 8: AT Program Coordination.

2.8.1. GCCs coordinate AT and security matters with the appropriate CoM and host-nation authorities for countries within their AOR and with the Heads of the other DOD Components whose personnel are stationed in or transit the respective GCC AOR.

2.8.2. AF Component commanders of personnel who will be stationed in or transit the AOR of a GCC shall:

2.8.2.1. Initiate coordination of AT matters with the appropriate GCC pursuant to the requirements established by DODD 2000.12. The senior deployed commander with AT responsibility will designate an ATO in writing to coordinate with the AF Component to the GCC and provide this information through the Unit Deployment Centers with Unit Type Codes (UTCs) assigned for the deployment. AF elements of in-transit forces with less than 300 personnel and not deploying as a larger troop movement will comply with the GCC operation order (OPORD) and file an in-transit AT plan. File in-transit AT plans with their ATO and commander for approval. Coordinate with AF Components to GCCs or MAJCOMs to determine in-transit AT plan filing requirements. The plan will cover travel from permanent station to the initial assembly or embarkation point, where it becomes the responsibility of the senior officer of a larger movement, such as a troop commander. If the movement does not join a larger force where AT responsibility is transferred, the AT plan must include transit to the deployed location where a commander is designated as having AT responsibility by orders. For countries where the AF will be performing temporary duty, commanders will immediately contact the AFOSI unit or ATO responsible for that AOR. AFOSI will provide a specific, tailored threat briefing prior to departure.

2.8.2.1. **(ACC)** AFOSI detachments will establish a procedure for providing threat briefings to deploying units.

2.8.2.2. To support AT planning and implementation, AT matters are coordinated with local, State, Federal and host-nation authorities pursuant to existing law, and AF and DOD policy.

2.8.3. Subordinate elements of the DOD Components on AF installations or self-supported separate facilities and AF tenant units on installations or self-supported separate facilities shall coordinate AT program and plan requirements with the host installation or self-supported separate facility commander or civilian equivalent director. Tenant units shall participate fully in installation and self-supported separate facility AT programs. At locations where there are multiple DOD components, such as DOD-leased facilities or other facilities where DOD occupies space, the designated senior DOD Component, unless otherwise stipulated by the applicable GCC, shall be responsible for integrating and coordinating individual DOD component security plans into a comprehensive installation, self-supported separate facility or area-wide AT program.

2.9. Standard 9: AT Officer (ATO).

2.9.1. Commanders will designate ATOs in writing (see Standard 26 for certification criteria). The ATO is the commander's military or civilian advisor charged with managing the AT Program. The ATO advisory role does not replace a functional manager's or commander's responsibility to execute programs in support of the operational commander's mission. Security clearance requirements will be established by the commander. ATOs shall be assigned to:

2.9.1.1. Installations or self-supported separate facilities with inherent responsibility for emergency response functions.

2.9.1.2. Wings and higher.

2.9.1.2. **(ACC)** For AT/FP issues pertaining to the installation, tenant wings, squadrons, etc., will be subordinate to the Installation ATO.

2.9.1.3. Squadrons having 100 or more personnel.

2.9.1.3. **(ACC)** All organizations on the installation with more than 100 personnel assigned, to include tenants and other DOD agencies, must appoint a primary and alternate unit ATO (UATO) in writing; individual must be an E-5 or above/or civilian equivalent. Wing and/or UATOs will complete an approved AT Level II training, and/or applicable AT refresher training. All UATO's will work with the Installation ATO for all AT/FP issues.

2.9.1.4. Deploying squadrons and higher with potential perimeter security and access control responsibilities.

2.9.1.5. Deploying units under the operational control of a designated commander having 300 or more personnel (both civilian and military) assigned.

2.9.2. All ATOs shall:

2.9.2.1. Assist the commander in implementing Joint, DOD, GCC and Air Force AT-related doctrine, policy and TTPs. Make recommendations to the commander if supplemental policy and guidance is necessary to execute the commander's AT Program.

2.9.2.2. Provide guidance, priorities and resourcing strategies for the correction or mitigation of AT vulnerabilities utilizing CVAMP.

2.9.2.3. Recommend CbT-RIF submissions to correct or mitigate emergency or emergent AT vulnerabilities through the AF Component to the GCC in accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5261.01F, *Combating Terrorism Readiness Initiatives Fund*.

2.9.2.4. Provide AT considerations, to include real-world and exercise lessons learned, into appropriate concept of operations and other procedural guidance.

2.9.2.5. Collaborate with the TWG to determine if action through warnings, policy and guidance or organize, train and equip functions are necessary based on worldwide terrorism incidents or threats.

2.9.2.6. Work closely with AFOSI and Security Forces to support and advocate the Air Force Eagle Eyes program.

2.9.3. The following are additional responsibilities for ATOs appointed based on paragraphs 2.9.1.1 (installation or self-supported separate facilities) and 2.9.1.2 (wings and higher):

2.9.3.1. The minimum grade of these ATOs shall be O-3, E-7, GS-12 or YA-02. At small units or deployed locations, where the rank requirements cannot be met, the priority for selecting an ATO should be based on AT expertise and certification.

2.9.3.2. ATOs will be assigned to the commander's immediate staff for unfettered access to the commander or a senior officer on the commander's immediate staff. For expeditionary units, the ATO is assigned to the headquarters staff of the senior commander assigned AT responsibility.

2.9.3.2.1. **(Added-ACC)** The installation ATO will report directly to the wing commander or vice commander as the wing commander's AT subject matter expert/advisor. An alternate should be permanently assigned to assist the installation ATO when possible. The primary installation ATO requires a Top Secret clearance; the alternate installation ATO requires at least a Secret clearance.

2.9.3.2.2. **(Added-ACC)** Identify primary and alternate ATO's by appointment letter to HQ ACC/A7SO within 30 days of appointment and/or commander change.

2.9.3.2.2.1. **(Added-ACC)** Appointment letter shall identify: NIPR/SIPRNET e-mail addresses, duty phone number, cell phone/pager number (if appl.), and graduation dates from both the AT/FP Level II and Security Engineering Design courses.

2.9.3.2.2.2. **(Added-ACC)** Identify authorized CVAMP administrators by name and authorized permissions (i.e. Commander permissions).

2.9.3.2.3. **(Added-ACC)** The installation ATO will be designated as the installation's primary CVAMP Administrator.

2.9.3.3. Ensure CVAMP is used to identify and track AT resourcing actions and appropriate vulnerabilities are submitted to the GCCs for funding assistance.

2.9.3.4. Ensure CVAMP is populated with AT-related assessment vulnerabilities in accordance with this instruction. Additional functional databases may be used for follow-on project information and tracking, but a reference note must be documented in the vulnerability observation within CVAMP. Coordinate with functional commanders to ensure AT-related vulnerabilities are entered in and decisions or actions are tracked in CVAMP. **Note:** Other databases may be used to manage the follow up action(s), but the initial vulnerability and the project identification code or numbers must be recorded and tracked in CVAMP.

2.9.3.5. Monitor Program Element Code (PEC) 28047 and coordinates funding for AT initiatives.

2.9.3.6. Facilitate the ATWG and ATEC.

2.9.3.7. Coordinate with FPI representatives to develop the commander's CCIRs and PIRs.

2.9.3.8. Coordinate with Exercise Evaluation Teams (EETs) or the ATWG for integrated multifunctional, interagency (local, state, federal), OCONUS – multinational, installation-wide AT exercises involving AT, EM and/or Medical response per functional guidance to test capabilities against adversary COA, e.g., force on force, TTPs. The ATO assists functional leads in executing required exercises and evaluation of AT-related capabilities.

2.9.3.9. Coordinate multifunctional teams of Subject Matter Experts (SMEs) when conducting AT assessments. In conjunction with functional commanders, provide countermeasure(s) solutions to correct or mitigate risk or recommend where the commander may assume risk.

2.9.3.9. **(ACC)** The installation ATO will ensure all appropriate assessments are conducted IAW established directives.

2.9.3.10. Assist CE in determining the design basis threat to meet AT construction standards based on local threats.

2.9.3.10. **(ACC)** Civil Engineers will assist/provide appropriate design specifications to the SFS and ATO for determining appropriate security criteria/needs IAW Unified Facilities Criteria (UFC) 4-020-01 *DOD Security Engineering Facilities Planning Manual*; and UFC 4-010-01*, DOD Minimum Antiterrorism Standards for Buildings*. The installation ATO will review and ensure all UFC requirements are included and documented/signed off.

2.9.3.11. A full-time multi-functional staff shall be designated, trained and resourced to support these ATOs in administering their respective AT programs. As a minimum, functional representatives will be designated in writing. **Note:** AT programs should be integrated with other FP programs and overarching efforts to achieve protection, such as critical infrastructure protection and continuity of operations; however AF CIP is a separate AF program and restraint should be exercised if these program responsibilities are added to ATO responsibilities without appropriate SME staff support.

2.9.3.12. **(Added-ACC)** The installation ATO will attend all appropriate meetings associated with the AT/FP program that affects the installation. NOTE: The Critical Asset Risk Management (CARM) [formally the critical infrastructure program (CIP)] is a separate AF Program. Where the installation ATO has been designated as the CARM POC, wings should consider requesting a manpower study to adjust for the increased workload.

2.9.4. The following are additional responsibilities for ATOs appointed based on paragraph 2.9.1.1 (installation or self-supported separate facilities):

2.9.4.1. In conjunction with other ATOs, unit AT representatives, functionals and SMEs, facilitate interaction for developing and implementing plans and programs that allows seamless capability application and resource deconfliction for contingency response and incident management. As a minimum, this includes the AT, CEMP 10-2, MCRP, IDP and Disease Containment Plan (DCP).

2.9.4.2. Provide oversight to wing/installation RAM programs.

2.9.4.3. **(Added-SHAWAFB)** Conduct semiannual meetings, as a minimum, with UATOs. The 20FW/CCFP will chair this meeting. UATO meetings will be conducted to facilitate crossfeed, distribute and record AT taskings and introduce new AT information.

2.9.4.4. **(Added-SHAWAFB)** Conduct annual program assistance visits (PAVs) of unit-level AT programs utilizing but not limited to the checklist in Attachment 10). The 20 FW/CCFP will maintain the schedule of PAVs and findings. Units requiring corrective actions will be suspensed to document corrective actions within 30 calendar days.

2.9.4.5. **(Added-SHAWAFB)** Develop UATO training curriculum.

2.9.4.5.1. **(Added-SHAWAFB)** Conduct training for newly assigned UATO on a recurring basis.

2.9.5. The following are additional responsibilities for ATOs appointed based on paragraphs 2.9.1.3 (squadrons over 100 personnel) and 2.9.1.4 (deploying squadrons) and responsibilities of Unit AT Representatives:

2.9.5.1. Ensure FPCONs are implemented and report status to the installation or self-supported separate facility ATO as prescribed in the installation or self-supported separate facility AT plan.

2.9.5.2. Participate in the ATWG and TWG.

2.9.5.3. Ensure functional TTPs and guidance are integrated with the installation or self-supported separate facility AT program.

2.9.5.4. Arrange for Level I - AT Awareness Training and pre-deployment country threat briefs if not provided through the Unit Deployment Center.

2.9.5.5. Assist in scheduling and tracking RAM implementation and provide this information to the installation or self-supported separate facility ATO as prescribed in local guidance.

2.9.5.6. Assist in developing and tracking in-transit AT plans (Standard 8).

2.9.5.7. **(Added-SHAWAFB)** Advise the unit commander on AT matters affecting the unit.

2.9.5.8. **(Added-SHAWAFB)** Act as the focal point for developing and justifying project information to mitigate unit AT vulnerabilities.

2.9.5.9. **(Added-SHAWAFB)** Maintain updated unit appointment letter, as outline in Attachment 7 Letter will be updated annually or as changes occur and filed in unit AT Program Book, with group ATO and 20 FW/CCFP.

2.9.5.10. **(Added-SHAWAFB)** Maintain a unit AT Program Book, as outlined in Attachment 10.

2.9.5.11. **(Added-SHAWAFB)** Develop and maintain a unit OI, as outlined in Attachment 7.

2.9.5.12. **(Added-SHAWAFB)** Review the unit AT OI annually or as changes occur, document the review and maintain the review in the unit program book.

2.9.5.13. **(Added-SHAWAFB)** Maintain a stockpile of JS Guide 5260, *Service Member's Personal Protection Guide: A Self-help Handbook to Combating Terrorism*, and the “Antiterrorism Individual Protective Measures” folding card.

2.9.5.14. **(Added-SHAWAFB)** Provide AT training statistics to the group ATO and 20 FW/CCFP as requested.

2.9.5.15. **(Added-SHAWAFB)** Ensure unit personnel receive Level I AT Awareness training annually.

2.9.5.16. **(Added-SHAWAFB)** Maintain an adequate supply of FPCON signs.

2.9.5.17. **(Added-SHAWAFB)** Conduct initial Physical Security Evaluations of each unit facility. Update annually or as needed. Documentation of the evaluations will be maintained in the unit AT Program handbook and a copy filed with the group and 20 FW/CCFP.

2.9.5.18. **(Added-SHAWAFB)** Ensure monthly RAM report is forwarded to the group ATO and 20FW/CCFP office.

2.10. Standard 10: AT Working Group (ATWG).

2.10.1. Multi-functional ATWGs shall be established at installations and self-supported separate facilities and higher (stationary and deployed) that meet at least semi-annually or more frequently, depending upon the level of threat activity. ATWGs oversee the implementation of the AT Program, develop and refine AT plans and address emergent or emergency AT program issues. The ATWG recommends COAs to the ATEC; develops AT-related policy, TTP and guidance; clarifies AT roles and responsibilities; conducts long-range planning and recommends resourcing requirements; and addresses emergent or emergency requirements through CbT-RIF.

2.10.2. ATWG membership shall include the ATO, the commander (or a designated representative), representatives of the principal staff, including persons with CBRNE expertise, tenant unit representatives and other representatives as required to support AT planning and program implementation. The chair and mandatory members of the ATWG will be designated in writing by the commander. Security clearance requirements for members will be established by the commander. An ATWG charter or similar document should be developed to describe member responsibilities and minimum functional and SME participation.

2.10.2.1. **(Added-ACC)** ACC has combined their antiterrorism (AT) and emergency management (EM) working groups to form the “ACC AT-EM WG”. NOTE: Installations should make every attempt to combine various wing working groups to ensure multifunctional representation and eliminate redundancy.

2.10.2.2. **(Added-ACC)** HQ ACC/A7S, or designated representative, chairs the ACC AT-EM WG, and keeps the Commander, Air Combat Command (COMACC) informed of all ACC AT-EM WG activities (via the AT executive committee). The ACC AT-EM WG is comprised of core members listed in the AT-EM WG charter. Each AT-EM WG member must possess a Secret clearance at a minimum.

2.10.2.3. **(Added-SHAWAFB)** At Shaw AFB the ATWG is comprised of representatives from the following organizations: 20 FW/CV (Chairperson), 20 FW/CCFP, 20 FW/XP, 20 FW/JA, 20 CPTS, 20 FW/PA, 20 OG, 20 MXG, 20 MDG, 20 MSG, 20 SFS, 20 CES, 20 CES/CEX, 20 CS, 20 OSS/IN, 20 SVS, AFOSI Det 212, 9AF, AAFES, DECA, AFAA, 372d Training Squadron (AETC), SMALC Depot Task Force, 682 Air Support Operations Squadron. Other specialties possessing AT functional expertise will participate in meetings as required. In order to ensure proper focus is placed on antiterrorism issues, the ATWG will remain a separate body from the Integrated Base Defense Working Group and the Emergency Management Working Group.

2.10.2.4. **(Added-SHAWAFB)** ATWG members will possess at a minimum a “SECRET” security clearance.

2.10.3. AF/A7SO chairs the Headquarters AF (HAF) FP Working Group.

2.11. Standard 11: Threat Working Group (TWG).

2.11.1. A multi-functional TWG shall be established at the installation and self-supported separate facilities and higher (stationary or deployed) that meet at least quarterly or more frequently, depending upon the level of threat activity. TWGs develop and refine terrorism threat assessments and coordinate and disseminate threat warnings, reports and summaries. The TWG reviews, coordinates and disseminates threat warnings, reports and summaries. They should consider terrorist threats and their asymmetrical methods of organization, intelligence, planning and operations that could pose a threat to the installation or operations in the Base Boundary and/or Base Security Zone (BSZ). They also track CBRN active defense warnings and intelligence community threat alerts and advisories regarding terrorist groups and analyze the applicability to the installation and its operations.

2.11.1.1. **(Added-SHAWAFB)** After analyzing the available intelligence, the TWG will recommend an appropriate FPCON posture and accompanying antiterrorism measures for mitigating threats to the 20 FW/CC.

2.11.1.2. **(Added-SHAWAFB)** Terrorism Threat Advisories, Terrorism Warning Reports, threat level changes and FPCON changes will be disseminated to 9AF, 20 MDG, 20 MSG, 20 MXG, 20 OG and all tenant units through the 20 FW/CP. Each group CC is responsible to disseminate this information to their respective units.

2.11.2. TWG membership shall include the ATO, the commander (or a designated representative), members of the staff, and appropriate representatives from tenant units, direct-hire, contractor, local, State, Federal, host-nation law enforcement agencies and the intelligence community. The chair and mandatory members of the TWG will be designated in writing by the commander. Security clearance requirements for members will be established by the commander. A TWG charter or similar document should be developed to describe member responsibilities and minimum functional and SME participation.

2.11.2. **(SHAWAFB)** TWG members will possess a minimum of a SECRET security clearance.

2.11.2.1. **(Added-ACC)** TWG membership at the installation/unit level will be comprised of AFOSI, SFS, intelligence, CARM program manager, and the ATO as minimum. Other members are (e.g. Civil Engineering Squadron Emergency Management Flight, Explosives Ordnance Disposal, Fire Department, Bio/Medical, etc.) should be added based on the threat.

2.11.2.1.1. **(Added-SHAWAFB)** The 20 SFS/CC will serve as the chairperson of the TWG.

2.11.2.2. **(Added-ACC)** AFOSI 2 FIR commander, or designated representative, chairs the HQ ACC TWG, and keeps the COMACC informed of all HQ ACC TWG activities. The ACC TWG core membership is comprised of representatives from the ACC A3 Operations Division (HQ ACC/A3O), HQ ACC/A7S, AFOSI Region 2, and 15 IS. The TWG meets to evaluate threats to ACC bases and make recommendations to ACC leadership as needed. Representatives from other functional areas requiring access to TWG meetings must have a Top Secret clearance. Representatives assigned to the ACC

TWG will have a Top Secret clearance and should complete an approved AT level II course.

2.11.2.3. **(Added-ACC)** The HQ ACC TIFC serves as the focal point for the collection, assessment and analysis of threat information relating to ACC personnel and resources and is operationally controlled by the AFOSI 2 FIR commander. When actionable intelligence is derived from ACC TIFC analysis, the information will be forwarded to the ACC TWG for action/awareness and/or disseminated to subordinate units throughout the command.

2.11.3. Based on threat information, appropriate SMEs shall be assembled to provide information needed to develop predictive intelligence and recommend COA to counter threats or otherwise reduce risk. If resources are available, especially at high threat locations or at MAJCOM or higher levels, members of the TWG may be further organized to form the basis of an Intelligence Fusion Cell as described in AFTTP 3-10.2, *Integrated Base Defense Command and Control.*

2.11.3.1. **(Added-SHAWAFB)** Threat Fusion Cell (TFC): 20 OSS/IN (strategic) – provides analytical support (trend analysis, products). AFOSI Det 212 (operational) – provides real-time assessments, liaison & direction. 20 SFS/S-2, Intelligence (tactical) coordinate & disseminate; implement FP measures. 20 FW/CCFP will be notified by the TFC during any situation that may need the assistance, or employment of the 20 FW TWG. At which point the TWG will be recalled and the TFC will brief the TWG on all pertinent data and the TWG will brief the 20 FW/CC on recommendation of implementation of transitional FPCONs or full FPCON implementation.

2.12. Standard 12: AT Executive Committee (ATEC).

2.12.1. An AT executive-level committee or similarly structured corporate body will be established at the installation and self-supported separate facility level and higher (stationary or deployed) that meets at least semi-annually. ATECs develop and refine AT program guidance, policy and standards; act upon recommendations of the ATWG and TWG; and determine resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities. The chair and mandatory members of the ATEC will be designated in writing. Security clearance requirements for members will be established by the commander. An ATWG charter or similar document should be developed to describe member responsibilities and minimum functional and SME participation.

2.12.1.1. **(Added-SHAWAFB)** The ATEC will be chaired by the 20 FW/CC or designated representative. Voting members will include FW/CV, OG/CC, MXG/CC, MSG/CC, MDG/CC and a (0-5/0-6) representative from 9 AF/USAFCENT. Non-voting members will consist of 20 SFS/CC, AFOSI Det 212/CC and 20 FW/CCFP. Other ATWG members may be present to discuss antiterrorism issues.

2.12.1.2. **(Added-SHAWAFB)** The ATEC will meet on a quarterly basis to ensure installation leadership remains abreast of status of AT plans, AT related exercises, AT-related memorandums of agreement (MOA) with off-base organizations, RAM program effectiveness, unit level support of base FPCON measures, and status of vulnerability mitigation efforts.

2.12.1.3. **(Added-SHAWAFB)** ATEC members will possess at a minimum a "SECRET" security clearance.

2.12.2. AF/A7S chairs the HAF FP Steering Group.

2.13. Standard 13: AT Physical Security Measure.

2.13.1. Principles of AFTTP 3-10.1, *Integrated Base Defense*, AFI 31-101 and DOD 5200.08-R, *Physical Security Program*, are applied and fully integrated into AT plans to ensure employment of a holistic security system to counter terrorist capabilities. Well-designed physical security measures are multi-layered and include the integration and synchronization of the following essential elements, as further described in DOD AT Standard 13: detection, assessment, delay or denial, communication and response. The development of comprehensive physical security measures requires the integration of facilities, physical security equipment, trained personnel, biometrics entry control equipment, when established, and procedures oriented at a minimum in support of perimeter and area security, access and egress control, protection against CBRNE attacks (including those using the postal system), HRP protection, barrier plans and facility standoff distances.

2.13.2. AOR or other mission-specific security policies are developed to guide subordinate development of local physical security systems and the purchase of physical security equipment.

2.13.3. Tenant command and unit security plans and measures are coordinated and integrated into the AT Plan.

2.13.3. **(ACC)** Where possible, installations are encouraged to cross reference between existing wing plans to eliminate conflicts of various functional responsibilities. DOD standards are compliance directives and are not waiver able.

2.13.4. Ensure barrier plans include measures to prevent reverse entry though exit lanes. Ensure the barrier plan affords personnel time to recognize a possible threat and employ the final barrier(s) while minimizing risk to vehicle occupants, e.g. placing a serpentine between the integrated defense (ID) check point and the final denial barrier. The purpose of the final denial barrier is to prevent an attack but planners must factor that most instances requiring barrier employment are because of mistakes in judgment by vehicle operators.

2.13.4.1. Barrier plans should protect facilities listed in the AT plan from vehicle attacks. Installations will ensure proper standoff through UFC and DOD O-2000.12-H recommended passive barriers. Barriers plans should also identify owner/users tasked with erecting barriers and specified time periods. See JP 3-07.02 for additional guidance on establishing barriers plans.

2.13.4.1.1. **(Added-ACC)** Barrier plans will be detailed to protect critical facilities from stationary vehicle attacks. The barrier plan critical facility list must be created from the criticality assessment. The UFC is the minimum baseline used for standoff to include barrier planning. Ensure documented design basis threat is utilized for any modifications.

2.13.4.1.2. **(Added-ACC)** CE is the OPR for the barrier plan, with SF and the installation ATO as office of collateral responsibility when establishing a barrier plan. Barrier plans, using UFC and traffic engineering standards, should be formally reviewed by the base Installation Security Council and/or the AT Working Group to ensure effectiveness, rapid deployment and where necessary, proper traffic redirection is needed.

2.13.4.1.3. **(Added-ACC)** Barrier plans will be referenced in the installation's AT plan.

2.13.5. **(Added-ACC)** CE flights will assist security forces and the installation ATO in providing programming and landscape support to place permanent barriers/standoff all the time, to minimize implementation time as threat increases. All new military construction/refurbishing of facilities will incorporate in-place barrier planning techniques.

2.14. Standard 14: Random Antiterrorism Measure.

2.14.1. The RAM program is developed and implemented as an integral component of the overall AT program and guided by the principles outlined in DOD O-2000.12-H. To maximize the effectiveness and deterrence value, RAMs should be implemented without a set pattern, either in terms of the measure selected, time, place or other variables. Lessons learned have highlighted unpredictability in security activities as one of the best and most cost effective deterrents available to a commander. Randomly changing AT TTPs enable integrated defenses to appear formidable and prevent threats from easily discerning and predicting patterns or routines that are vulnerable to attack. RAMs, at a minimum, shall consist of the random implementation of higher FPCON measures, to include MAJCOM or locally developed site-specific measures, in consideration of the local terrorist capabilities. Random use of other security measures should be used to supplement FPCON measures. The RAM program shall be included in AT plans.

2.14.1.1. **(Added-ACC)** Random Antiterrorism Measures (RAM) shall employ elements of information warfare, as required, to support Air Force antiterrorism measures. If military deception and/or operations security are deemed necessary, contact the host unit's military deception office and the OPSEC office for assistance in development of tactical deception and OPSEC measures.

2.14.1.2. **(Added-ACC)** The installation ATO is responsible for managing the RAM program.

2.14.1.2.1. **(Added-SHAWAFB)** Publish a monthly Random Antiterrorism Measure (RAM) schedule through the 20 FW/CC or CV and distribute the schedule to group/unit ATOs.

2.14.2. When developing and implementing an effective installation RAM process:

2.14.2.1. Include tenant units and tenant commands.

2.14.2.2. Implement daily RAMs to include weekends and holidays. The frequency will be increased as the threat increases. At least three RAMs chosen from higher FPCONs are required daily.

2.14.2.3. Use RAMs to mitigate vulnerabilities impacting facilities and nearby areas.

2.14.2.4. RAM implementation should be compatible and coordinated with ongoing law enforcement or CI surveillance detection and ID measures.

2.14.2.5. Consider methods to make RAMs visible to confuse or expose surveillance attempts and preoperational planning.

2.14.2.6. Implement dynamic and proactive RAMs to communicate unit resolve to detect, deter, prepare for and counter threats.

2.14.2.7. Make efforts to include, as appropriate local, State, Federal and host nation law enforcement patrols and first responders.

2.14.2.8. Implement RAMs installation wide or target specific types of facilities, functions or activities.

2.14.2.9. RAM implementation efforts shall be monitored, tracked and analyzed.

2.14.2.9. **(ACC)** RAM tracking documentation will be maintained for a minimum of one (1) year.

2.14.2.9.1. **(Added-SHAWAFB)** UATOs will forward monthly RAM performance reports to their respective group ATO, reporting on 20 FW RAMs conducted, outlining all lessons learned, and highlighting areas of suggested improvement. If a RAM was not conducted, units will annotate reasons why and, as a minimum, review their current plan and indicate if the antiterrorism measure is contained in their unit AT OI/Unit-Specific FPCON Checklists. Use the format outlined in Attachment 12 to submit lessons learned.

2.14.2.9.2. **(Added-SHAWAFB)** The 20 FW/CCFP will compile all information and include it as part of the brief to the 20 FW/CC.

2.15. Standard 15: AT Measures for AF Off-Installation Facilities, Housing and Activities.

2.15.1. For AF owned or leased off-installation facilities, housing, transportation services, daycare centers and other activities used by or involving a mass-gathering of DOD personnel and their family members, specific AT measures shall be developed in overall AT programs. At locations where there are multiple DOD components or locations, AT measures shall be coordinated with the designated senior DOD Component with AT responsibility.

2.15.1.1. Risk mitigation measures shall include, but are not limited to: emergency notification and recall procedures, guidance for selection of off-installation housing, temporary billeting and other facility use (including compliance with UFC 4-010-01 for leased, newly constructed and expeditionary buildings), physical security measures, CBRNE defensive measures and shelter-in-place, relocation and evacuation procedures.

2.15.1.1. **(ACC)** Residential security reviews for off-installation housing will be based on the local threat assessment/level, not the national threat assessment.

2.15.2. Mutual Aid Agreements or other similarly structured protocols are developed with the appropriate local, State, Federal and host-nation authorities to coordinate security measures and assistance requirements.

2.16. Standard 16: AT Measures for High-Risk Personnel (HRP).

2.16.1. AT measures are developed pursuant to the principles outlined in DOD O-2000.12-H, DODI O-2000.22 and AFI 71-101, vol 2, *Protective Service Matters,* for personnel designated as HRP.

2.16.1.1. SAF/IGX is the HAF focal point for policy development and coordination with the OASD for Special Operations and low-Intensity Conflict and Interdependent Capabilities (OASD (SO/LIC&IC)) to implement DODI O-2000.22.

2.16.1.2. AFOSI is designated a PPO and is the AF lead for Protective Service Details (PSDs) and PSVAs.

2.16.2. Designation of positions as High-Risk Billets (HRB) and HRP shall be in accordance with DODI O-2000.22 and AFI 71-101, vol 2.

2.16.2.1. SAF/IGX shall staff nomination packages for the Secretary of the Air Force (SECAF), who will make the decision to nominate AF officials to the Office of the Secretary of Defense (OSD).

2.16.2.2. SAF/AA shall staff nomination packages for the AF Top-4 as appropriate.

2.16.2.3. Nomination packages shall be staffed through the appropriate MAJCOM or AF Component to a GCC.

2.16.3. AFOSI will complete a PSVA for each person occupying an HRB who is nominated for HRP in accordance with DODI O-2000.22 and AFI 71-101, vol 2. PSVAs will be initiated within 90 days of an individual’s assignment to an HRB and nomination for HRP. PSVA will be revalidated annually and updated if the TTL changes, but no less than every 3 years.

2.16.4. HRP and family members, as appropriate, shall complete appropriate high-risk training (personal protection, evasive driving, AT awareness and hostage survival); shall be properly cleared for assignment to positions, facilities or countries requiring such protection; and shall be thoroughly indoctrinated on the duties and responsibilities of protective service personnel.

2.16.5. HRP designees and their family members shall be familiar with treaty, statutory, policy, regulatory and local constraints on the application of supplemental security measures for certain high-ranking DOD officials who are provided additional protection due to their position.

2.16.6. HRP security measures shall be reviewed within 60 days of changes to the TTL for the affected country and HRP.

2.16.7. The provisions of AFI 23-302, *Vehicle Management*, shall be complied with for the acquisition and use of non-tactical armored vehicles.

2.17. Standard 17: AT Construction and Building Considerations.

2.17.1. All new construction and renovations, regardless of the funding source, that exceed 50 percent of the replacement cost or change the use of the facility must comply with UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*. Refer to AFPD 31-1, AFI 31-101, AFI 65-601, Vol 1, *Budget Guidance and Procedures*, and AFH 32-1084, *Facility Requirements*, for additional information. Proper facility project planning, programming and design must be done in concert with the ATO, installation intelligence and security personnel to adequately address site specific threats. Ensure restoration and modernization projects which include security and AT Standards compliance upgrades do not exceed 70 percent cost versus new facility standard.

2.17.1.1. The installation commander or the senior Civil Engineer on the commander's behalf will certify that new facility or renovation projects of 50 percent or more of replacement cost comply with standards as listed in paragraph 2.17.1. The ATO will work with the engineering staff from design inception to project completion, ensuring requirements are met. The ATO should be part of the coordination prior to certification. The senior Civil Engineer will report discrepancies to the appropriate MAJCOM for determination/action.

2.17.1.1. **(ACC)** The installation ATO will be part of the coordination prior to certification to ensure compliance with appropriate UFC and security engineering requirements.

2.17.1.1.1. **(Added-SHAWAFB)** The 20 CES/CC and Chief Engineer will certify in a written memorandum that all new construction projects meet or exceed the standards contained in the Unified Facilities Criteria. 20 CES will utilize the format in Attachment 13 when developing the certification memorandum.

2.17.1.2. **(Added-ACC)** In addition to UFC 4-010-01, all new construction and renovations, regardless of the funding source, that exceed 50 percent of the replacement cost or change the use of the facility must comply with UFC 4-020-01, *DOD Security Engineering Facilities Planning Manual*, and UFC 4-010-02, *DOD Minimum Antiterrorism Standoff Distances for Buildings.*

2.17.2. Ensure the A7 (CE) and ATO develop a prioritized list of risk mitigation measures (reference DOD O-2000.12-H, UFCs and AFI 31-101) for use by site selection teams. These criteria shall be used to determine if facilities either currently occupied or being considered for occupancy provide adequate protection for DOD personnel against the effects of a terrorist attack. Circumstances may require the movement of DOD personnel or assets to facilities the U.S. Government had not previously used or surveyed. AT Standards shall be a key consideration in evaluating the suitability of facilities that were previously not used or surveyed.

2.17.3. The A7 (CE) will ensure at least one engineer at each installation has completed the Security Engineering and Design Course to review, document and track construction projects for compliance with UFCs and AT Standards.

2.17.3. **(ACC)** Installation ATOs will attend the Security Engineering Design course and include the date of attendance (or scheduled date) on the appointment letter.

2.18. Standard 18: AT Measures for Logistics and Other Contracting.

2.18.1. AT measures shall be incorporated into the logistics and contracting processes (requirements development, vendor selection, award, execution and evaluation) when the provisions of the contract or services provided affect the security of DOD elements, personnel, mission-essential cargo, equipment, assets or services. When commensurate with risk, consider AT performance as an evaluation factor for contract award (past performance and proposed performance under the instant contract) and as a performance metric under the resultant contract.

2.18.2. A verification process, whether through background checks or other similar processes shall be implemented to enable the U.S. Government to attest to the trustworthiness of DOD contractors and sub-contractors (U.S. citizens, host-nation and third country personnel) to the greatest extent possible, including those personnel having direct or indirect involvement in the delivery or provision of services. Priority will go to service provisioning related to mail and food, water or other materiel intended for consumption by DOD personnel. This vetting of trustworthiness shall include agents and crews on contracted ships, planes, trains and overland vehicles. Refer to AFI 31-101.

2.18.2.1. **(Added-ACC)** Installations should refer to DTM (I) 09-012 (DOD Physical Access Control) and DOD 5200.08-R, *Physical Security Program*, for types of check to be conducted.

2.18.2.2. **(Added-ACC)** The base contracting officer shall ensure criminal background checks, as appropriate, are accomplished prior to employment. Incorporate Air Force Federal Acquisition Regulation Supplement (AFFARS) 5352.242-9000, *Contractor Access to Air Force Installations*, into local contracts. Contracting will ensure statements of work include security and force protection provisions designed to ensure contractor compliance with the implementation of higher FPCONs, including subcontractor compliance.

2.18.2.2. **(SHAWAFB)** All contracts effecting classified work will be coordinated through 20 FW/IP.

2.18.3. Site-specific risk mitigation measures are developed and implemented to maintain positive control of DOD contractor and sub-contractor access to and movement within installations, sensitive facilities and classified areas.

2.18.4. Site-specific risk mitigation measures are developed and implemented to screen contractor or sub-contractor transportation conveyances for CBRNE hazards before entry into or adjacent to areas with DOD personnel and mission-essential assets.

2.18.5. Contracts will comply with the AT provisions of the Defense Federal Acquisition Regulation.

2.18.6. Contracts shall incorporate Level I - AT Awareness Training requirements. See Standard 25.

2.19. Standard 19: AT Measures for Critical Asset Security.

2.19.1. Risk management measures shall be developed to reduce the vulnerabilities of DOD assets assessed as critical in STANDARD 5, to include distributive information or computer-based systems and networks. Integrate these measures into overall AT program efforts.

2.19.2. Coordinate with appropriate local, State, Federal or host-nation authorities responsible for the security of non-DOD assets deemed essential to the functioning of DOD assets assessed as critical.

2.20. Standard 20: Terrorism Incident Response Measures.

2.20.1. Incident response measures shall be developed consistent with the principles outlined in DOD 5200.08-R and AFI 10-2501 and included in the overall AT plan. These measures shall include procedures for determining the nature and scope of incident response (including incidents with a CBRNE component); procedures for coordinating security, fire, medical, hazardous material and other emergency responder capabilities; and steps to recover from the incident while continuing essential operations.

2.20.1. **(ACC)** Ensure all wing plans are consistent with all applicable DOD standards i.e.; AFI 10-2501, *Air Force Emergency Management (EM) Program Planning and Operations*; AFI 14-119, *Intelligence Support to Force Protection*; and AFI 31-101, *Integrated Defense*; and the medical community instructions.

2.20.2. AF Components to GCC or GCCs prepare incident response measures for their AOR. AFOSI and Force Protection Detachments should be included in contingency planning for in-transit units.

2.21. Standard 21: Terrorism Consequence Management Measures.

2.21.1. Consequence management, CBRNE and public health emergency preparedness and emergency response measures are included as an adjunct to the overall AT Plan or installation emergency management plans. For the AF these measures are found in the CEMP 10-2, MCRP, AT Plan and the IDP. The contents of all plans may be referenced in the AT Plan. These measures shall focus on mitigating vulnerabilities of personnel, families, facilities and materiel to terrorist use of WMD and CBRNE weapons, as well as overall disaster planning and preparedness to respond to a terrorist attack. These measures shall include integration with DOD emergency responder guidelines provided in AFI 10-2501; mass notification system standards under UFC 4-021-01; establishment of medical surveillance systems consistent with DODD 6490.02E, *Comprehensive Health Surveillance*, and AFI 10-2604, *Disease Containment Planning Guidance*; deployment of CBRNE sensors and detectors; providing collective protection; and providing personal protective equipment (PPE) or individual protective equipment (IPE) in the following priority and in accordance with AFI 10-2501. The contract Statement of Work or Performance Work Statement must specify if PPE will be government or contractor provided:

2.21.1.1. First Responders and Emergency Responders. Personnel who work closest to known or suspected CBRNE hazards (e.g., emergency responders) should be provided protection needed to perform their duties in an unknown hazard environment. Responders should use the maximum possible protection until determined otherwise by competent authority.

2.21.1.2. Critical Personnel. Personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, host-nation personnel or third country nationals), such as critical personnel assigned to mission essential functions (MEFs) described in AFI 10-208, *Continuity of Operations Program (COOP)*, should be provided an appropriate level of protection to support continuity of those critical military missions. Since critical missions should be continued without interruption, collective or individual protection may be necessary to sustain them.

2.21.1.3. Essential Personnel. Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, host-nation personnel or third country nationals) should be provided an appropriate level of protection to support near continuity for those essential military operations. Since essential operations may be interrupted for relatively short periods (e.g., hours to days), escape protection may be necessary to sustain essential operations (i.e., escape, survive and restore essential operations).

2.21.1.4. Other Personnel. For all other persons not in the above categories, the objective will be to provide the procedures or protection necessary to safely survive an incident, e.g. shelter-in-place or evacuation procedures may fulfill this requirement.

2.21.1.5. Included as part of the above categories are those who work or live on DOD installations worldwide, family members authorized overseas and DOD contractors if designated in contract agreements and designated as essential to perform critical DOD missions.

2.21.2. Site-specific CBRNE preparedness and emergency response measures are developed and coordinated through the Readiness and Emergency Management Flight. These measures are implemented and synchronized with a corresponding FPCON measure.

2.21.3. Mutual Aid Agreements or other similarly constructed protocols will be established with the appropriate local, State, Federal or host-nation authorities to support AT Plan execution and augment incident response and post-incident consequence management activities.

2.21.3. **(ACC)** Installation ATO will ensure functional compliance for all appropriate memorandums of agreement/understanding.

2.21.4. The installation should be able to warn its resident population in affected areas of possible or confirmed CBRNE hazards immediately, utilizing the Air Force Installation Notification and Warning System (INWS). The warning must include instructions to shelter in place or evacuate.

2.21.5. Installation public health emergency response measures that are synchronized with FPCON levels shall be developed and implemented.

2.21.6. **(Added-ACC)** Weapons of Mass Destruction (WMD) detection strategies should be multi-functional in approach. CE Readiness and Emergency Management and Explosives Ordnance Disposal (EOD) will be the OPR for developing criteria for the selection of WMD detection equipment, including developing maintenance, training, and employment plans. As the incident dictates, the installation ATO should be included in the Crisis Action Team (CAT) and Emergency Operations Center (EOC) functions as an advisor to the commander.

2.22. Standard 22: Force Protection Condition (FPCON) Measures.

2.22.1. The GCC is responsible for establishing the baseline FPCON for their AOR and procedures to ensure that FPCON measures are uniformly disseminated and implemented. The AF Component to the GCC is typically delegated to manage this task for the GCC. See Attachment 2 for detailed listing of FPCON measures.

2.22.2. Installation commanders with AT responsibility and higher shall:

2.22.2.1. Determine an appropriate FPCON level for those personnel and assets for which they have AT responsibility. Subordinate commanders may raise a higher-level commander’s FPCON level, but they shall not lower the FPCON level without the higher-level commander’s written concurrence.

2.22.2.1.1. **(Added-ACC)** Installation command posts will ensure proper OPREP-3 reporting procedures [and will info Air Forces North Security Forces Division (AFNORTH A7S OMB)] reporting of any FPCON changes.

2.22.2.1.2. **(Added-ACC)** FPCON Measure Deviations. The inability to meet minimum DOD and Air Force installation antiterrorism requirements results in a higher force protection program risk. If it is determined certain mandated FPCON measures are inappropriate for current operations or negatively impact threat mitigation efforts, installation commanders may request a waiver in writing through their respective chain of command to the respective FPCON declaring authority. The waiver request will address the specific FPCON measure in question, the proposed action, efforts to mitigate related vulnerabilities, and plans for the installation to come into compliance with the mandated FPCON measure. Ensure proper classification requirements are met. Approval can only be granted by the declaration authority. Deviations must be staffed through HQ ACC/A7S.

2.22.2.2. Classify site-specific AT measures and physical security actions, linked to an FPCON as “CONFIDENTIAL”. When separated from the AT Plan, specific AT measures linked to a FPCON and site-specific FPCON levels may be downgraded to “FOR OFFICIAL USE ONLY,” in accordance with DOD 5200.1-R, *Information Security Program*.

2.22.2.2. **(ACC)** Non-ACC tenant organizations on ACC installations must comply with local AT programs.

2.22.3. A review mechanism is established to ensure FPCON levels are commensurate with changing threats and the principles of risk management. This is essential because implementation of FPCON measures at elevated FPCON levels for an extended duration can be counterproductive to effective security and overall mission accomplishment. In some circumstances, based upon local conditions and the threat environment, commanders should consider implementing a lower-level FPCON and supplement with other local security measures and RAMs as an effective alternative to executing the higher-level FPCON measures.

2.22.4. Site-specific FPCON measures are developed and implemented for stationary and in-transit forces to supplement the FPCON measures and actions enumerated for each FPCON level. The development of site-specific FPCON measures must permit sufficient time and space to determine hostile intent, while fully considering constraints imposed by standing rules of engagement in CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules For the Use of Force For U.S. Forces,* and rules of force under AFI 31-207, *Arming and Use of Force by Air Force Personnel*. Organic intelligence, CI and law enforcement resources, institutional knowledge of the area and comprehensive understanding of organic capabilities, supported by national and AOR assets, shall be leveraged in directing tailored FPCON measures to be implemented at specific sites for both stationary and in-transit forces.

2.22.4.1. **(Added-SHAWAFB)** Unit commanders will outline in their AT OI any unique procedures and resources necessary to comply with the DoD FPCON measures, as well as developing any unit-specific FPCON measures necessary to ensure the security of their facilities and resources.

2.22.4.2. **(Added-SHAWAFB)** Unit ATOs will forward unit-specific FPCON measures to the 20 FW/CCFP, who will in turn compile a base-wide list of site-specific FPCON measures.

2.22.5. **(Added-SHAWAFB)** FPCON signs, SHAWAFBVAs 31-18 through 31-25, (See Figure1.1. below) indicating the current Real World and Exercise FPCON levels will be posted at the necessary entrances/exits to manned facilities on Shaw Air Force Base. FPCON signs are not required for emergency exits or other entrances/exits not used for normal day-to-day operations. Note: Units will identify in writing the entrances/exits for posting FPCON signs and maintain the list in the unit AT program book IAW Attachment 11 . FPCON signs will be clearly displayed at eye level on necessary entrances/exits doors, with the Real World sign posted on the left side of door and Exercise sign posted on the right side of door. Additionally, SHAWAFBVA 31-27, *Be Alert and Report*, signs will be displayed in place of (over) exercise FPCON signs when there is not an exercise in effect.

2.22.5.1. **(Added-SHAWAFB)** Facilities will be marked using Real world SHAWAFBVA 31-18 through SHAWAFBVA 31-21 signs and Exercise SHAWAFBVA 31-22 through 31-25, and SHAWAFBVA 31-27 signs maintained on the Shaw Air Force Base Publishing web accessible from the “Shaw Intranet” under the “Publications” link. Signs will be on the appropriate stock paper and posted using 8 ½ x 11 clear document protectors. The following are the approved Shaw AFB signs and corresponding FPCON.

2.22.5.1.1. **(Added-SHAWAFB)** SHAWAFBVA 31-18, *FPCON ALPHA*

2.22.5.1.2. **(Added-SHAWAFB)** SHAWAFBVA 31-19, *FPCON BRAVO*

2.22.5.1.3. **(Added-SHAWAFB)** SHAWAFBVA 31-20, *FPCON CHARLIE*

2.22.5.1.4. **(Added-SHAWAFB)** SHAWAFBVA 31-21, *FPCON DELTA*

2.22.5.1.5. **(Added-SHAWAFB)** SHAWAFBVA 31-22, *EXERCISE FPCON ALPHA*

2.22.5.1.6. **(Added-SHAWAFB)** SHAWAFBVA 31-23, *EXERCISE FPCON BRAVO*

2.22.5.1.7. **(Added-SHAWAFB)** SHAWAFBVA 31-24, *EXERCISE FPCON CHARLIE*

2.22.5.1.8. **(Added-SHAWAFB)** SHAWAFBVA 31-25, *EXERCISE FPCON DELTA*

2.22.5.1.9. **(Added-SHAWAFB)** SHAWAFBVA 31-27, *Be Alert and Report*

2.22.5.1.10. **(Added-SHAWAFB)** Worn signs will be replaced as needed.

2.22.6. **(Added-SHAWAFB)** The 20 FW/CC through the 20 FW/CP will utilize all available communications media (e.g., Telephone, NIPRNET, SIPRNET, Giant Voice) to disseminate changes to the FPCON condition. The specific antiterrorism measures to be implemented will be outlined via Battle Staff Directive.

Figure 2.2. (Added-SHAWAFB) Real World FPCON Sign

Figure 2.3. (Added-SHAWAFB) Exercise FPCON Sign

Figure 2.4. (Added-SHAWAFB) Be Alert sign

2.23. Standard 23: AT Training and Exercises.

2.23.1. AT training and exercises shall integrate with physical security and relevant elements of AT, EM, FHP and ID and are afforded the same emphasis as combat task training and executed with the intent to identify shortfalls affecting the protection of personnel, assets and information against terrorist attack and subsequent AT consequence management efforts.

2.23.2. AT and AOR specific training, particularly pre-deployment training, is supported by measurable standards, including credible deterrence and response standards, deterrence-specific TTPs and lessons learned. AT training shall also be incorporated into unit-level training plans and pre-deployment exercises. Pre-deployment training shall also include terrorism or similarly designed scenarios and hostile intent decision making. Joint operations and exercises shall incorporate AT training and planning for forces involved.

2.23.3. At least annually, comprehensive field and staff training, including deploying squadrons and higher, are conducted to exercise AT plans. Annual AT exercises shall encompass all aspects of AT, physical security and emergency management plans. Additionally, current baseline FPCON through FPCON CHARLIE measures shall be exercised annually at installations and self-supported separate facilities.

2.23.3. **(ACC)** AT exercises will have maximum participation by all base units, including tenant units, with a minimum of simulation. Wings should make every effort to use local community first responders for this exercise. AT exercise scenarios may be held in conjunction with other Air Force required exercises (e.g., HAZMAT, Force-on-Force, Mass Casualty, etc.) to meet various Air Force instruction requirements. Each AT exercise will be documented by the base exercise evaluation team, providing a critique with findings, observations, and lessons learned.

2.23.4. Maintain AT exercise documentation for no less than 2 years to ensure incorporation of lessons learned.

2.23.4.1. **(Added-SHAWAFB)** 20 FW/XPI will maintain the master copy of exercise reports. Reports will be reviewed at subsequent ATWG meetings.

2.23.5. AT lessons learned are submitted through the AF Lessons Learned program and, when appropriate, through the Joint Lessons Learned program.

2.23.5. **(ACC)** AT lessons learned are submitted through the Air Force Lessons Learned program at **https://www.jllis.mil/usaf**/.

2.23.6. ATOs in coordination with the Wing EET shall develop a comprehensive annual training and exercise program to provide the necessary individual and collective training to prepare for an annual exercise.

2.23.6.1. **(Added-SHAWAFB)** The 20 FW/CCFP office is the OPR for AT exercises. Exercises will be coordinated with 20 FW/XP. The complete AT plan and a Weapons of Mass Destruction scenario will be exercised at least annually.

2.23.6.1.1. **(Added-SHAWAFB)** During Phase I planning, 20 FW/XPI, 20 FW/CCFP and AFOSI will develop plausible exercise intelligence designed to elevate the installation's FPCON level to at least BRAVO. Phase I exercises should include an evaluation of the TWG decision-making process and the installation's ability to effectively deter terrorist incidents.

2.24. Standard 24: Formal AT Training.

2.24.1. The AF's formal AT Training Program shall consist of Level 1 - AT Awareness Training (Standard 25), Level II - ATO Training (Standard 26), Level III - Pre-command AT Training (Standard 27), Level IV - AT Executive Seminar (Standard 28), AOR-specific training (Standard 29) and HRP AT training (Standard 16).

2.24.2. AT training shall be integrated into officer, NCO and civilian training as required by this Instruction and whenever possible and appropriate. Long term improvement and implementation of effective AT programs depends upon a solid training foundation for all grades, skills and functional areas.

2.24.2.1. All AF assigned personnel shall complete appropriate formal AT training and education. Individual permanent records shall be updated to reflect completion of the training.

2.24.2.2. ATOs and unit personnel are encouraged to attend additional protection related courses, e.g., Security Engineering and Design Course.

2.24.2.2. **(ACC)** Installation ATOs will attend the Security Engineering Design course and include the date of attendance (or scheduled date) on the appointment letter.

2.24.2.3. Required AT formal training shall be provided to individuals who are not properly trained upon arrival to a new assignment or as soon as possible. Report AF training deficiencies through the AF chain of command to the appropriate MAJCOM. Report other Service training discrepancies through the appropriate AF Component to the GCC.

2.25. Standard 25: Level I - AT Awareness Training.

2.25.1. Every military Service member, DOD employee and local national or third country citizen in a direct-hire status by the DOD, regardless of grade or position, shall complete Level I - AT Awareness Training requirements.

2.25.2. DOD contractors shall be provided AT information as required by DFAR, Section 252.225-7043. Level I - AT Awareness Training shall be offered to DOD contractor employees under the terms and conditions as specified in the contract, especially when the performance is OCONUS. The TWG should determine the best method to offer training to contractor employees.

2.25.3. Dependent family members ages 14 years and older traveling OCONUS on official business (e.g., on an accompanied permanent change of station move) shall complete Level I - AT Awareness Training as part of their pre-departure requirements.

2.25.3.1. Commanders will encourage dependent family members to complete Level I - AT Awareness training before any personal travel OCONUS (e.g., leave) or to any locale where the TTL is MODERATE or higher.

2.25.4. Level I - AT Awareness Training shall be provided in initial entry basic training or in general military subject training for all initial entry AF military and civilian personnel. AF personnel accessions must receive this initial training under the instruction of a qualified Level I - AT Awareness Training instructor.

2.25.5. All individuals qualified to administer Level I - AT Awareness Training will be designated in writing. Individuals who complete a formal AF approved Level II - ATO Training (Standard 26) course of instruction, whether in residence or through a mobile training team, may qualify to administer Level I - AT Awareness training.

2.25.5. **(SHAWAFB)** All personnel who have graduated from AT Level II training will be considered qualified to administer Level I.

2.25.5.1. If a certified instructor is not available, as an interim solution, commanders will certify and appoint qualified SMEs (e.g., security forces, special agents, EM, Bioenvironmental Engineer, intelligence personnel) who have received formal training in AT TTP and individual security and protection, and are knowledgeable in the current AT publications and methods for obtaining AOR-specific updates. Commanders must clearly describe the qualifications of the individual in the appointment letter to justify this method and explain why other options are not feasible.

2.25.6. Individuals completing Level I - AT Awareness Training shall:

2.25.6.1. Have the requisite knowledge to remain vigilant for possible terrorist actions.

2.25.6.2. Be capable of employing AT TTP as outlined in DOD O-2000.12-H.

2.25.7. Level I - AT Awareness Training is built upon the minimum requirements outlined in DODI 2000.16, Standard 25, Table E3.T2. Table 2.2 below supplements DOD Standard 25 with AF modifications. AT Awareness training offered by other Services or DOD agencies meets AF requirements as long as they fulfill all requirements of DOD Standard 25.

Table 2.2. Minimum AT Awareness Training Requirements.

AT Awareness instruction shall include at least the following subjects (AF added/modified): - Personal protective measures for CBRNE attacks utilizing local or theater specific emergency management guidance and procedures - Force Health Protection measures

2.25.8. Annually, post-accession Level I - AT Awareness Training shall be provided to all AF personnel. Annual post-accession Level I - AT Awareness Training may be accomplished by one of two means:

2.25.8.1. Instruction from a qualified Level I AT Awareness Training instructor.

2.25.8.2. Completion of a DOD or AF-sponsored and certified computer or web-based distance learning instruction. **Note:** AF personnel assigned or attached to an embassy on

TDY under CoM authority must receive Level I – AT Awareness Training from a qualified instructor.

2.25.9. HQ AF Security Forces Center (AFSFC/SFOZ) is responsible for managing the AF Level I - AT Awareness Training.

2.25.10. AF assigned personnel complete Level I – AT Awareness Training as part of the AF annual ancillary training program.

2.25.10.1. The Force Support Squadron will document Level I - AT Awareness Training for individuals and their dependents that are 14 years or older. This training requirement will be included in the relocation process. Training must be completed prior to final out-processing.

2.25.10.2. Orders approving officials and/or Unit Deployment Managers (UDM) shall document completion of Level I - AT Awareness and AOR specific training on OCONUS deployment orders.

2.25.10.3. Unit Training Managers document Level I - AT Awareness Training with the date of completion in Military Modernization Personnel Data System (MILPDS). If MILPDS is unavailable, Unit Training Managers will document AT Awareness Training through normal ancillary records. Unit Training Managers will provide Level I - AT Awareness Training status and statistics upon request.

2.25.10.4. Aircrews will document their Level I - AT Awareness Training as ARMS Code G110 (Level I - AT Awareness Training).

2.26. Standard 26: Level II - ATO Training.

2.26.1. Individuals will be qualified as an ATO by completion of a formal AF approved Level II - ATO Training course of instruction, whether a course in residence or through a mobile training team. At permanent duty locations, newly assigned, uncertified ATOs shall complete a formal AF approved Level II - ATO Training course within 120 days of appointment. At temporary duty locations the most expedient arrangements shall be used to send a trainee to formal training.

2.26.1. **(ACC)** Individuals requiring seats in the ACC AT level II school will contact the ACC Security Forces training team (HQ ACC/A7STT) at **acc.a7stt@langley.af.mil** for quotas.

2.26.2. AF approved Level II - ATO Training courses are listed in Attachment 5. Level II - ATO Training shall prepare ATOs to manage AT programs, advise the commander on all AT issues, qualify individuals to administer Level I - AT Awareness Training and coordinate support required for completion of Level I - AT Awareness Training.

2.26.3. Certified ATOs shall remain current and proficient.

2.26.3.1. Personnel who are qualified as an ATO but have not served as an ATO in the last 12 months shall complete a formal AF approved Level II - ATO refresher training course of instruction. The refresher may be through a course in residence, mobile training team or computer or web-based distance learning instruction.

2.26.3.2. Personnel who are qualified as an ATO but have not served as an ATO in the last 13 months to 3 years shall re-attend a formal AF approved Level II - ATO Training course of instruction. The refresher may be through a course in residence or mobile training team.

2.26.4. MAJCOMs with Level II - ATO Training courses shall:

2.26.4.1. Designate course of instruction requirements for ATO personnel.

2.26.4.1.1. **(Added-ACC)** The 99th Security Forces Group (SFG) AT Level II course cadre will provide a proposed calendar year schedule for the new fiscal year to HQ ACC/A7STT NLT September 1st. The schedule will include annual Nellis-based course offerings to be advertised Air Force and DOD-wide. Mobile Training Team (MTT) will be scheduled with all ACC bases to ensure Level II MTT training on a biannual basis. Additional MTTs and Nellis-based courses will be added as the schedule and cadre manning permits.

2.26.4.1.2. **(Added-ACC)** Installation ATOs will submit names of attendees to HQ ACC/A7STT 30 days prior to the class start date (CSD) for all Nellis based or MTT courses. All updates/changes to the attendee rosters must be coordinated through the installation ATO. The installation ATO will make contact with HQ ACC/A7STT NLT 7 days prior to CSD to provide final attendee roster detailing all changes/updates. HQ ACC/A7STT will load attendees through the Air Force Personnel Center into Oracle Training Administration (OTA), and a student roster will be pulled by 99 SFG cadre NLT 3 days prior to CSD. Installation ATOs are also responsible for ensuring the training site meets MTT support specifications.

2.26.4.2. For new courses, submit a Plan of Instruction (PoI) to HQ AFSFC/SFOZ for approval prior to initiating any training. PoIs will be submitted to HQ AFSFC/SFOZ as requested.

2.26.4.2. **(ACC)** The 99 SFG AT Level II course cadre will provide a draft lesson plan on an annual basis to HQ ACC/A7SO NLT October 1st.

2.26.4.3. Command-specific requirements may be added to the core curriculum. Develop measurable standards for Level II - ATO Training and determine evaluation methods to ensure trainees are proficient.

2.26.4.4. Conduct an annual review of Level II - ATO Training course curriculum to validate minimum curriculum content.

2.26.4.5. Maintain a reference library of all AT-related publications relevant to the course of instruction.

2.26.4.6. Develop an AF Form 797, *Qualification Standard Continuation/Command Job Qualification Standard(JQS)*, to task certify personnel serving as instructors, as appropriate.

2.26.4.7. Establish a PDS Code of “AFI” to identify Level II - ATO Training courses.

2.26.4.8. Review potential instructor candidates to ensure prerequisites are met prior to commencement of duties.

2.26.5. Personnel serving as Level II - ATO Training course instructors will, as a minimum, have completed the following:

2.26.5.1. A formal AF instructor’s course, such as Principles of Instruction, Academic Instructor School, Basic Instructor Course, etc. The Principles of Instruction course is the minimum required standard. Personnel may begin instructing students without having completed this requirement provided they have a certified instructor serving as the Supervising Instructor. However, they are required to have a date to attend one of the above courses within 90 days of being assigned instructor duties.

2.26.5.2. Graduate from an AF approved Level II - ATO Training course (Attachment 5).

2.26.5.3. Be task certified on an AF Form 797, as appropriate.

2.26.5.4. Instructors should expand their AT knowledge by attending courses such as sister Service AT training, Dynamics of International Terrorism (DIT) and CVAMP training. Additionally, conducting over-the-shoulder observations of HHA VAs adds to credibility and subject matter expertise.

2.26.5.4. **(ACC)** In addition, 99 SFG AT level II instructors should attend the US Army’s Protective Design Centers *“Security Engineering Design Course.”*

2.26.5.5. Level II - ATO Training instructors should have had 2-years field experience as an ATO.

2.26.6. Level II - ATO Training is built upon the minimum requirements outlined in DODI 2000.16, Standard 26, Table E3.T3. Table 2.3 below supplement DOD Standard 26 with AF modifications. The AF developed Level II - ATO Training courses can be specialized, but every course must cover either the installation (I) or deployable unit (U) joint requirements, at a minimum.

Table 2.3. Minimum Level II - ATO Training Requirements.

1. (I/U) Complete a formal AF-approved Level II - ATO Training course of instruction, whether a course in residence or through a mobile training team (CONUS or OCONUS).
2. (I/U) Level II - ATO Training shall consist of the following minimum topics (AF added):
a) (I/U) Understanding FP Roles and Responsibilities
- (I/U) Understand necessary Host Nation and Civil Support Agreements and Requirements
b) (I/U) Prepare AT Plans (consider using the JAT Guide)
- (U) How to Integrate AT Plans with CEMP 10-2, MCRP, IDP, etc.
3. (I/U) Review of the following DOD and Joint Staff publications (AF added).
a) (I/U) UFCs 4-010-01, 4-010-02, 4-020-01fa, 4-020-03fa, 4-020-04fa, 4-022-01, 4-023-03 and 4-021-01
b) I) Agile Combat Support Concept of Operations
c) (I) AFDD 2-4.1, *Force Protection*
d) (I/U) AFTTP 3-10.1, *Integrated Base Defense*
e) (I/U) AFTTP 3-10.2, *Integrated Base Defense Command and Control*
f) (I/U) AFI 10-245, *Antiterrorism (AT)*
g) (I/U) AFI 10-2501, *AF Emergency Management (EM) Program Planning and Operations*
h) (I) AFI 10-2603, *Emergency Health Powers on Air Force Installations*
i) (I) AFI 10-2604, *Disease Containment Planning Guidance*
j) (I/U) Air Force Lessons Learned Program
k) (I/U) AFI 14-119, *Intelligence Support to Force Protection*
l) (I/U) AFI 31-101, *The Air Force Installation Security Program*
4. (I/U) If available, add the following to Level II - ATO Training courses:
a) SME presentations from the Federal Bureau of Investigations (FBI), AFOSI, EOD, Intel, Medical Group, etc.
b) Hands-on instruction of Antiterrorism Enterprise Portal (ATEP) and CVAMP

2.27. Standard 27: Level III - Pre-command AT Training.

2.27.1. Squadron, group and wing commanders (O-5 or O-6 commanders and civilian equivalent director position) shall complete Level III - Pre-command AT Training before assuming command.

2.27.2. MAJCOMs will ensure this training is provided to squadron commanders, e.g. during MAJCOM squadron commander orientation seminars or other means. Group and wing commanders will receive this training through the group and wing commander courses. MAJCOMs will determine minimum qualifications for personnel delivering Level III - Pre-command AT Training.

2.27.2.1. **(Added-ACC)** HQ ACC/A7SO is the office of primary responsibility (OPR) for AT Level III training and provides the required training during the ACC Squadron Commanders' course.

2.27.2.2. **(Added-ACC)** Installation ATOs will provide AT Level III briefings to all commanders who arrive on station without having attended the ACC Squadron Commanders Course. HQ ACC/A7SO will provide standardized Level III curriculum slides to installation ATOs upon request to conduct the training.

2.27.3. Level III - Pre-command AT Training is built upon the requirements outlined in DODI 2000.16, Standard 27, Table E3.T4. Table 2.4 below supplement DOD Standard 27 with AF modifications. A minimum of a 1-hour block is provided to properly address the minimum topics. Additionally, commanders are encouraged to attend the Joint Special Operations School's "*Commander's Responsibility Course, Antiterrorism and Force Protection.*"

2.27.3.1. Installation commanders are required to gain a thorough understanding of all the requirements.

2.27.3.2. All other commanders are required to gain a thorough understanding of all requirements not marked with an asterisk. Asterisk designated requirements only require introduction, which at a minimum will include explanatory remarks and sufficient reference material for commanders to complete their AT responsibilities.

Table 2.4. Minimum Level III - Pre-command AT Training Requirements.

1. Pre-Command AT training shall include the following minimum topics (AF added/modified):

a) Understanding AT responsibilities and minimum AT Program Elements

- Risk Management and Risk Assessments

b) * Ensuring preparation of AT plans

- Baseline FPCON posture

- Integrated Defense Plan

- Mitigating CBRNE, WMD attack and risks in support of EM plans

- MOUs, Memorandums of Agreement (MOAs) and MAAs

- JAT Guide Capabilities

c) * Organization of AT groups

- ATWG

- TWG

- ATEC

d) *Understanding the local threat picture

- Potential sources of law enforcement-derived Force Protection information

- Fusion of Intelligence, CI and law enforcement information

- Terrorism Threat Levels

e) *How the installations integrate with the National Response Framework

f) *How the installation integrates with the Country Team

2. Review of references includes GCC OPORDs (AF added).

2.28. Standard 28: Level IV - AT Executive Seminar.

2.28.1. Commanders at all echelons will ensure appropriate military officers in the grades of O6 through O8 and civilian equivalent/senior executive service civilian employees attend the AT Executive Seminar as described in DOD Standard 28.

2.28.2. The AT Executive Seminar is administered by the Joint Staff (J-3 Deputy Director for AT/Homeland Defense, J34). Nomination requests are sent through the Services and COCOMs.

2.28.3. The AT Executive Seminar provides DOD senior military and civilian executive leadership with the requisite knowledge to enable development of AT Program policies and facilitate oversight of all aspects of AT programs at the operational and strategic levels.

2.28.3. **(ACC)** The ACC Senior Leader Management Office (HQACC/A1L) is the OPR for ACC seats to AT Level IV courses.

2.29. Standard 29: Area of Responsibility (AOR)-Specific Training for DOD Personnel and In-transit Forces.

2.29.1. GCCs develop and provide AOR specific training and provide in-transit forces with threat information. The AT awareness training and education programs orient all DOD personnel with AOR-specific information on AT protection. This AOR-specific information is in addition to annual Level I - AT Awareness Training and may be provided through multiple means, including GCC/AF Component to the GCC/MAJCOM publications, messages, Internet Web sites, AFI 24-405 and DOD 4500.54-M.

2.29.2. AF personnel (including family members ages 14 years and older) departing to another GCC's AOR shall complete the gaining GCC's, AF Component to the GCC's or MAJCOM's AOR-specific AT education requirements within 3 months of a permanent change of station.

2.29.2. **(ACC)** Family members can obtain country information at **http://travel.state.gov/travel/cis_pa_tw/cis/cis_1765.html**. Geographic Combatant Commander information can be gathered on their respective SIPRNet website.

2.29.3. Commanders of AF in-transit forces, units and individuals will obtain from GCCs, AF Component to the GCCs or MAJCOMs detailed threat information covering transit routes and sites that will be visited by the deploying unit or individuals. Such information includes focused information on potential terrorist threats (e.g., tailored production and analysis) and guidance on the development of AT protection risk mitigation measures to aid in the development of tailored AT planning. Similar tailored information is also provided to intra-theater transiting units and individuals.

2.29.4. **(Added-ACC)** AFOSI is the office responsible for providing appropriate threat briefings. However, wing intelligence units may provide threat briefings if a memorandum of understanding is signed between the local AFOSI detachment and the intelligence unit detailing this sharing or shifting of responsibility between the detachment and the unit. Briefers should have attended Dynamics of International Terrorism and/or AT/FP Level II training, when possible. Unit deployment managers will annotate/track compliance.

2.30. Standard 30: AT Resource Application.

2.30.1. Risk shall be assessed against the standard and mitigation measures applied. Where the resulting risk is still deemed too great, the countermeasure requirement shall be elevated using the PPB&E process. Where applicable and in accordance with the MOU between the Department of State (DOS) and the DOD, *Overseas Security Support,* coordination will be made through MAJCOMs or AF Components to GCCs with the appropriate GCC to ensure that resource requirements for AT programs are identified and programmed. See Attachment 4 for more information on AT resourcing.

2.30.2. For emergent or emergency AT requirements that could not reasonably have been anticipated or programmed, prioritization shall be coordinated with the appropriate GCC, AF Component to the GCC or MAJCOM and CbT-RIF requests shall be submitted to the Chairman of the Joint Chiefs of Staff (CJCS) as specified in CJCSI 5261.01E. AF

Components to the GCC or MAJCOMs will submit CbT-RIF through the GCC. GCCs forward CbT-RIF requests to the CJCS using CVAMP.

2.30.2.1. **(Added-SHAWAFB)** The 20 FW/CCFP will compile background information for Combating Terrorism Readiness Initiative Fund (CBTRIF) submissions and forward them as directed by HQ ACC/SFOF.

2.30.2.2. **(Added-SHAWAFB)** The 20 FW RA will coordinate spending of awarded money with the 20 FW/CCFP and provide documentation to identify what was purchased and ensure funds were spent properly. The 20 FW/CCFP will track all AT spending and will report expenditures to ACC/SFO with supporting documentation, upon request.

2.30.3. MAJCOMs will submit validated prioritized AT resource requests with compelling justification, including those submitted or considered for CbT-RIF, to the GCC for review and submission to the CJCS on an annual basis pursuant to current DOD Program Objective Memorandum (POM) guidance and timelines using CVAMP.

2.30.4. Tenant units on AF installations and facilities shall coordinate and prioritize AT program and resource requirements according to PPB&E procedures with the host installation commander, applicable Military Department and appropriate GCC.

2.30.5. Antiterrorism PEC 28047F is the primary funding source for manpower authorizations, AT equipment, procurement, and the associated costs specifically identified and measurable to those resources and activities associated with the Air Force AT Program. AF/A7SX is the AF Program Element Monitor (PEM).

2.30.5.8. **(SHAWAFB)** (Added) All Shaw Air Force Base units will provide AT funding requirements to the 20 FW/CCFP with a full purchasing package as soon as requirements are identified and paperwork is completed.

2.30.5.9. **(Added-SHAWAFB)** The 20 FW/CCFP will submit a package to the ATWG to review and prioritize the wing vulnerabilities listing. Funding requests will be reviewed by the ATEC and approved by 20 FW/CC in order to meet ACC suspense’s.

2.30.5.1. **(Added-ACC)** AT funds (PEC 28047) will be dispersed to primarily mitigate or correct vulnerabilities/concerns identified during vulnerability assessments and loaded in CVAMP. UFR submissions will be the primary source for AT funding data calls.

2.30.5.2. **(Added-ACC)** CVAMP administrators will work with CE programmers and/or SMEs, to ensure UFRs are correctly inputted with appropriate cost information.

2.30.5.3. **(Added-ACC)** CE programmers will provide cost data to ATO for inclusion into CVAMP entries for those vulnerabilities requiring projects and/or minor construction. This also includes AT/FP projects in ACES.

2.30.5.4. **(Added-ACC)** Consider organizing an installation Vulnerability Action Group (VAG) to provide a multifunctional approach to track, mitigate, prioritize, and advocate for funding to close base vulnerabilities; and report its progress to the AT-EM WG. If utilized, a VAG should have representation from the ATO, CARM, CE Programming and Readiness, Communications, Comptroller, Operations, Security Forces, and Surgeon General.

2.30.5.5. **(Added-ACC)** AT/FP projects will be incorporated into the wing integrated priority list for funding consideration. Wing leadership must emphasize appropriate prioritization for the program.

2.30.5.6. **(Added-SHAWAFB)** The future year Financial Plan (FinPlan) is the avenue to identify valid funding requests into the MAJCOM's Program Objective Memorandum (POM) process. During the first quarter of each year, 20 CPTS will be tasked by MAJCOM to submit the wing FinPlan. 20 CPTS will send out a message with specific guidance to all group Resource Advisors (RA) requesting unfunded requirement submissions. One element of this request is for AT program requirements for the next fiscal year. This submission includes the dollar amount, full description of request and impact if request is not funded. The Unit Antiterrorism Officer (UATO) will submit AT requests through their respective group RA, back to 20 CPTS for official wing FinPlan submission to MAJCOM.

2.30.5.7. **(Added-SHAWAFB)** Funding submissions will be justified using DoD directives, AF directives and higher headquarter and local Vulnerability Assessment findings.

2.31. Standard 31: Comprehensive AT Program Review.

2.31.1. Comprehensive AT program reviews are conducted to evaluate the effectiveness and adequacy of AT program implementation. The evaluation shall include an assessment of the degree to which Air Force AT programs comply with the standards prescribed in this Instruction. AT program reviews shall evaluate all mandatory AT program elements (DOD Standard 1) and assess the viability of AT plans (DOD Standard 7) in view of local operational environment constraints and conditions. DOD O-2000.12-H provides procedures and recommendations to conduct comprehensive AT Program reviews. Other procedures include reviewing AT programs based on JSIVA or AFVAT benchmarks or DOD AT Strategic goals.

2.31.2. Comprehensive AT program reviews shall be conducted at least annually by all commanders required to establish AT programs.

2.31.3. Comprehensive AT program reviews shall be conducted in conjunction with pre-deployment VAs (Standard 6).

2.31.3.1. The purpose of a pre-deployment AT program reviews is to ensure that deploying units have viable AT programs and executable AT plans for transit to, from and during operations or training exercises in the deployed AOR.

2.31.3.2. Deploying AF elements shall comply with the GCC's AT guidance.

2.31.4. A comprehensive AT program review shall be conducted whenever there are significant changes in threat, vulnerabilities or asset criticality.

2.31.5. MAJCOMs shall ensure subordinate commands undergo an external AT program review at least once every 3 years. The ultimate outcome of triennial AT program reviews is the identification of AT program deficiencies that may be exploited by terrorists. The AT program review teams should provide realistic solutions aimed at improving AT program implementation and risk mitigation strategies.

2.31.5.1. Triennial AT program reviews may be conducted as an HHA or JSIVA. The AF may use an HHA or JSIVA in lieu of an annual AT program review.

2.31.5.2. In addition to providing an assessment of compliance with the AT Standards, an HHA or JSIVA shall assess and evaluate the viability of a headquarters' AT policies, subordinate AT program implementation, the methodology for addressing resource shortfalls, inter-organization coordination and synchronization of AT program elements.

2.31.6. Tenant commands and units located on AF installations shall be included in comprehensive AT program reviews.

2.31.7. **(Added-SHAWAFB)** The 20 FW/CCFP will publish a Program Assistance Visit (PAVs) checklist. 20 FW/CCFP will schedule and conduct reviews of unit programs annually. PAVS will also be conducted during Major AT Exercises by EET.

2.31.7.1. **(Added-SHAWAFB)** Items rated as "NOT COMPLIANT" will require monthly written updates until the item is determined to meet minimum compliance. The format in Attachment 14 will be used to report and track non-complaint items.

2.31.7.2. **(Added-SHAWAFB)** Program review reports and required monthly updates will be coordinated through the appropriate command channels and filed with the 20 FW/CCFP.

2.32. Standard 32: AT Program Review Teams.

2.32.1. AT program review assessment team guidelines shall be modeled upon the *DTRA AT VA Team Guidelines* and include, at a minimum, compliance with the standards prescribed in this Instruction, accepted TTPs and best AT practices.

2.32.2. A sufficient number of AT program review teams shall be resourced to execute the program review assessment requirements of the AF and to ensure AT program review teams comprise of individuals with sufficient functional expertise to assess and evaluate satisfactorily the effectiveness and adequacy of AT Program implementation at the level for which the AT Program review is being conducted (headquarters, unit, command, installation, activity, etc.).

2.32.2.1. **(Added-SHAWAFB)** AFOSI Det 212 and 20 FW/CCFP are tasked to evaluate items under the Terrorist Operations portion of the Vulnerability Assessment, in coordination with 20 OSS/IN.

2.32.2.2. **(Added-SHAWAFB)** Security Operations Specialist Benchmarks. 20 SFS is the lead agency tasked to evaluate benchmarks under this tab during the vulnerability assessment. 20 SFS will evaluate benchmarks EM-PLN-09 (Security Forces [SF] Terrorist Incident Response [TIR] Measures), EM-PLN-16 (Security Forces Emergency Response Equipment), SO-PLN-10 (Security Force Equipment), SO-PLN-11 (Entry Control Procedures) and EM-PLN-09 (Security Forces Terrorist Incident Response Measures).

2.32.2.3. **(Added-SHAWAFB)** Benchmarks: 20 CES is the lead agency tasked to assess benchmarks under the Structural Engineering, Infrastructure Engineering and Emergency Management tabs. 20 CES will evaluate benchmark IE-PLN-20 (Fire Protection), EM-PLN-08 (Fire Department Terrorist Incident Response Measures).

2.32.2.4. **(Added-SHAWAFB)** 20 LRS will evaluate the Bulk Fuel benchmarks contained under the Infrastructure Engineering Tab of the AF Benchmarks

2.32.2.5. **(Added-SHAWAFB)** 20 MDG will evaluate benchmarks EM-PLN-10 (Medical [MED] Terrorist Incident Response [TIR] Measures), EM-PLN-14 (Mass Casualty Planning), EM-PLN-17 (Medical Emergency Response Equipment) and EM-RM-04 (Food VA).

2.32.2.6. **(Added-SHAWAFB)** 20 CS will evaluate benchmark EM-PLN-19 (Mail Facility Response Measures and other Command, Control, Communications, and Computers (C4) Benchmarks.

2.32.2.7. **(Added-SHAWAFB)** 20 FW/PA will evaluate benchmark EM-PLN-23 (Public Affairs Officer[PAO])

2.32.2.8. **(Added-SHAWAFB)** Installation Antiterrorism Operations Benchmarks. 20 FW/CCFP will be the lead agency tasked to assess benchmarks under this tab during the vulnerability assessment.

2.33. (Added-ACC) AT Recognition Program Awards.

2.33.1. **(Added-ACC)** HQ ACC will follow the same AT award program formats as used by DOD and HQ USAF. The ACC Installations and Mission Support Directorate (HQ ACC/A7) will forward specific details and a notification message for annual award submissions to ACC units each year.

2.33.2. **(Added-ACC)** HQ ACC/A7 will forward all winning packages to the Air Staff for inclusion in the Air Force competition.

DANIEL J. DARNELL, Lt Gen, USAF
DCS/Air Space and Information Operations, Plans and Requirements

(ACC)

RICHARD J. WHEELER, Colonel, USAF
Deputy Director, Air Combat Command
Installations and Mission Support

(SHAWAFB)

CHARLES L. MOORE, JR., Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFDD 2-4.1, *Force Protection*, 9 November 2004

(Added-SHAWAFB) AFMAN 33-363, Management of Records, 1 March 2008

(Added-SHAWAFB) JS Guide 5260, Service Member's Personal Protection Guide: A Self-help Handbook to Combating Terrorism

(Added-SHAWAFB) SHAW AFB OPLAN 10-245, Installation Antiterrorism Plan, 1 July 2011

(Added-SHAWAFB) SHAWAFBVA 31-18, FPCON ALPHA, 18 April 2007

(Added-SHAWAFB) SHAWAFBVA 31-19, FPCON BRAVO, 18 April 2007

(Added-SHAWAFB) SHAWAFBVA 31-20, FPCON CHARLIE, 18 April 2007

(Added-SHAWAFB) SHAWAFBVA 31-21, FPCON DELTA, 18 April 2007

(Added-SHAWAFB) SHAWAFBVA 31-22, EXERCISE FPCON ALPHA (color Black, White and Red), 18 April 2007

(Added-SHAWAFB) SHAWAFBVA 31-23, EXERCISE FPCON BRAVO (color Black, White and Red), 18 April 2007

(Added-SHAWAFB) SHAWAFBVA 31-24, EXERCISE FPCON CHARLIE (color Black, White and Red), 18 April 2007

(Added-SHAWAFB) SHAWAFBVA 31-25, EXERCISE FPCON DELTA (color Black, White and Red), 18 April 2007

(Added-SHAWAFB) SHAWAFBVA 31-27, Be Alert and Report Sign (color Black, White and Red), 23 January 2008

AFPD 10-24, *Air Force Critical Infrastructure Program*, 28 April 2006

AFPD 10-25, *Emergency Management*, 26 September 2007

AFPD 10-26, *Counter-Chemical, Biological, Radiological and Nuclear Operations,* 26 September 2007

AFPD 31-1, *Integrated Defense,* 7 July 2007

AFPD 71-1, *Criminal Investigations and Counterintelligence,* 1 July 1999

AFI 10-208, *Continuity of Operations Program (COOP),* 1 December 2008

AFI 10-246, *Food and Water Protection Program,* 4 December 2004

AFI 10-2501, *Air Force Emergency Management (EM) Program Planning and Operations,* 24 January 2007

AFI 10-2603, *Emergency Health Powers on Air Force Installations*, 7 December 2005

AFI 10-2604, *Disease Containment Planning Guidance*, 6 April 2007

AFI 14-119, *Intelligence Support to Force Protection (FP)*, 15 August 2007

AFI 23-302, *Vehicle Management*, 29 October 2007

AFI 24-405, *Department of Defense Foreign Clearance Guide*, 6 May 1994

AFI 31-101, *The Air Force Installation Security Program*, 1 March 2003

AFI 31-207, *Arming and Use of Force by Air Force Personnel*, 29 January 2009

AFI 33-200, *Information Assurance (IA) Management*, 23 December 2008

AFI 38-201, *Determining Manpower Requirements*, 30 December 2003

AFI 65-601volume 1, *Budget Guidance and Procedures*, 3 March 2005

AFI 71-101volume 1, *Criminal Investigation*, 1 December 1999

AFI 71-101volume 2, *Protective Service Matters*, 18 November 2002

AFI 90-201, *Inspector General Activities*, 22 November 2004

AFH 10-2401, *Vehicle Bomb Mitigation Guide* (FOUO), 1 September 2006

AFH 32-1084, *Facility Requirements*, 1 September 1996

AFMAN 10-2602, *Nuclear, Biological, Chemical, and Conventional (NBCC) Defense Operations and Standards*, 29 May 2003

AFTTP 3-10.1, *Integrated Base Defense*, 20 August 2004

AFTTP 3-10.2, *Integrated Base Defense Command and Control*, 1 March 2008

AFTTP 3-10.3, *Integrated Defense Counterthreat Operations (CTO)*, 22 December 2008

CJCS Guide 5260, *Antiterrorism Personal Protection Guide: A Self-Help Guide to Antiterrorism*, 1 February 2008

CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules For the Use of Force For U.S. Forces* (available on SIPR at **www.js.smil.mil/masterfile/sfsimd/jel/index.htm**)

CJCSI 5261.01F, *Combating Terrorism Readiness Initiatives Fund*, 21 October 2008

CJCS Pocket Card 5260, *Antiterrorism Individual Protective Measures*, 1 October 2001

DODD 2000.12, *DOD Antiterrorism (AT) Program*, 18 August 2003

DODD 3020.40, *Defense Critical Infrastructure Program (DCIP)*, 19 August 2005

DODD 4500.54-M, *DOD Foreign Clearance Manual (FCM)*, 16 December 2008 (**https://www.fcg.pentagon.mil/fcg.cfm**)

DODD 6490.02 E, *Comprehensive Health Surveillance*, 21 October 2004

DODI 2000.16, *DOD Antiterrorism (AT) Standards*, 2 October 2006; change 2, December 8, 2006

DODI O-2000.22, *Designation and Physical Protection of DOD High-Risk Personnel (HRP)*, 22 January 2008

DODI 4525.8_AF Supplement 1, *DOD Official Mail Management*, 20 March 2006

DODI 5210.89_AFI 10-3901, *Minimum Standards for Safeguarding Biological Select Agents and Toxins,* 24 September 2007

DODI 5240.18, *Counterintelligence Analysis and Production,* 4 December 2006

DOD O-2000.12-H, *Antiterrorism Handbook,* 1 February 2004

DOD O-2000.12-P, *Department of Defense Antiterrorism Strategic Plan,* 1 June 2004

DOD 5200.1-R, *Information Security Program*, 14 January 97

DOD 5200.08-R, *Physical Security Program*, 9 April 2007

DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons,* 1 December 1982

(Added-ACC) DTM (I) 09-012, *DOD Physical Access Control/DOD 5200.08-R Physical Security,* 8 December 2009

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 30 May 2008

JP 3-07-2, *Antiterrorism*, 14 April 2006

UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*, 8 October 2003

UFC 4-010-02, *DOD Minimum Antiterrorism Standoff Distances for Buildings*, 8 October 2003

(Added-ACC) UFC 4-020-01, *DOD Security Engineering Facilities Planning Manual*, 11 September 2008

UFC 4-021-01, *Design and O&M: Mass Notification Systems*, 18 December 2002

Agile Combat Support Concept of Operations, October 1999

Defense Federal Acquisition Regulation Supplement (DFARS), 20 October 2008

Defense Threat Reduction Agency, *Antiterrorism Vulnerability Assessment Team Guidelines*, March 1, 2002

Defense Threat Reduction Agency (JSIVA) Security Classification Guide 6 May 2005

Homeland Security Presidential Directive 5, 28 February 2003

Homeland Security Presidential Directive 8, 17 December 2003

National Response Framework, January 2008

Protection Joint Functional Concept, June 2004

Adopted Forms.

AF Form 797, *Job Qualification Standard Continuation/Command JQS*

AF IMT 847, *Recommendation for Change of Publication*

(Added-ACC) UFC 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*, 25 May 2005

Unified Command Plan, 5 May 2006

(Added-SHAWAFB) DD Form 2637, *Physical Security Evaluation Guide (Stocked & Issued By OASD (FM&P)(SO/LIC/CT)*

Abbreviations and Acronyms

(Added-SHAWAFB) FinPlan— Financial Plan

(Added-SHAWAFB) ACC—Air Combat Command

(Added-SHAWAFB) AF—Air Force

AF CIP—Air Force Critical Infrastructure Program

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

(SHAWAFB) AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

(SHAWAFB) AFPD—Air Force Policy Directive

(Added-SHAWAFB) AFRIMS—AF Records Information Management System

AFSFC—Air Force Security Forces Center

AFTTP—Air Force Tactics, Techniques and Procedures

AOR—Area or Responsibility

AT—Antiterrorism

(SHAWAFB) AT—Antiterrorism

(ACC) AT-EMWG—Antiterrorism-Emergency Management Working Group

ATEC—Antiterrorism Executive Committee

(SHAWAFB) ATEC—Antiterrorism Executive Committee

ATO—Antiterrorism Officer

(SHAWAFB) ATO—Antiterrorism Officer

ATWG—Antiterrorism Working Group

(SHAWAFB) ATWG—Antiterrorism Working Group

BSAT—Biological Select Agents and Toxins

(Added-ACC) 2 FIR—2nd Field Investigations Region

(Added-SHAWAFB) C4—Command, Control, Communications and Computers

(Added-ACC) CARM—Critical Asset Risk Management

(Added-SHAWAFB) CBTRIF—Combating Terrorism Readiness Initiative Fund

C-NAF—Component-Numbered Air Force

CBRNE—Chemical, Biological, Radiological, Nuclear and high-yield Explosive

CbT—Combating Terrorism

CbT-RIF—Combating Terrorism Readiness Initiatives Fund

CCIR—Commander's Critical Information Requirements

CEMP—Comprehensive Emergency Management Plan

C&I—Communications and Information

CI—Counterintelligence

CJCS— Chairman of the Joint Chiefs of Staff

CJCSI— Chairman of the Joint Chiefs of Staff Instruction

COA—Course of Action

CoM—Chief of Mission

CONOPS—Concepts of Operations

CTO—Counterthreat Operations

CVAMP—Core Vulnerability Assessment Management Program

DCIP—Defense Critical Infrastructure Program

DCP—Disease Containment Plan

DFAR—Defense Federal Acquisition Regulation

DIA—Defense Intelligence Agency

DOD—Department of Defense

(SHAWAFB) DOD—Department of Defense

DODD—Department of Defense Directive

DODI—Department of Defense Instruction

DOS—Department of State

DRU—Direct Reporting Units

DTA—DOD Threat Assessment

EET—Exercise Evaluation Team

EM—Emergency Management

EOD—Explosive Ordnance Disposal

FHP—Force Health Protection

FOA—Field Operating Agency

FP—Force Protection

FP—Force Protection Detachment

FPCON—Force Protection Condition

(ACC) FPCON—Force Protection Condition

(Added-SHAWAFB) FPEC—Force Protection Executive Council

FPI—Force Protection Intelligence

GCC—Geographic Combatant Commander

GSU—Geographic Separated Unit

HHA—Higher Headquarters Assessment

HAF—Headquarters Air Force

HN—Host Nation

(Added-ACC) HQ ACC/A30—ACC A3 Operations Division

(Added-ACC) HQ ACC/A3OH—ACC Homeland Defense Branch

(Added-ACC) HQ ACC/A7—ACC Installations and Mission Support Directorate

(Added-ACC) HQ ACC/A7S—ACC Security Forces Division

(Added-ACC) HQ ACC/A7SO—ACC Security Forces Operations Branch

(Added-ACC) HQ ACC/A7STT—ACC Security Forces Training Team

HRB—High-Risk Billet

HRP—High-Risk Personnel

(Added-SHAWAFB) IAW—In Accordance With

ID—Integrated Defense

IDP—Integrated Defense Plan

IED—Improvised Explosive Device

IPE—Individual Protective Equipment

JAT—Joint Antiterrorism Guide

JP—Joint Publication

JSIVA—Joint Staff Integrated Vulnerability Assessment

MAA—Mutual Aid Agreement

MAJCOM—Major Air Command

MCRP—Medical Contingency Response Plan

(Added-SHAWAFB) MED—Medical

MEF—Mission Essential Functions

MILCON—Military Construction

NAF—Numbered Air Force

OASD—Office of the Assistant Secretary of Defense

OCONUS—Outside the Continental United States

(Added-SHAWAFB) OI—Operating Instruction

OPCON—Operational Control

OPORD—Operation Order

OPR—Office of Primary Responsibility

(SHAWAFB) OPR—Office of Primary Responsibility

PA—Public Affairs

(Added-SHAWAFB) PAO—Public Affairs Office

(Added-SHAWAFB) PAV—Program Assistance Visits

PEC—Program Element Codes

PHEO—Public Health Emergency Officer

PIR—Priority Intelligence Requirement

POM—Program Objective Memorandum

(SHAWAFB) POM—Program Objective Memorandum

PPB&E—Planning, Programming, Budgeting and Execution

PPO—Protection Providing Organization

PPE—Personal Protective Equipment

PSVA—Personal Security Vulnerability Assessment

RAM—Random Antiterrorism Measure

(SHAWAFB) RAM—Random Antiterrorism

(Added-SHAWAFB) RDS—Records Disposition Schedule

RED HORSE—Rapid Engineer Deployable Heavy Operations Repair Squadron

(Added-SHAWAFB) SF—Security Forces

SME—Subject Matter Expert

SOFA—Status of Forces Agreement

TACON—Tactical Control

(Added-SHAWAFB) TFC—Threat Fusion Cell

TIC—Toxic Industrial Chemical

(Added-ACC) TIFC—Threat Information Fusion Cell

TIM—Toxic Industrial Material

TTL—Terrorism Threat Level

TTP—Tactic, Technique and Procedure

TWG—Threat Working Group

(SHAWAFB) TWG—Threat Working Group

(Added-SHAWAFB) UATO—Unit Antiterrorism Officer

(Added-SHAWAFB) UCF—Unified Facilities Criteria

UCP—Unified Command Plan

UFC—Unified Facilities Criteria

(ACC) UFC—Unified Facilities Criteria

(Added-ACC) UFR—Unfunded Request

UTC—Unit Type Codes

VA—Vulnerability Assessment

VBIED—Vehicle Born Improvised Explosive Device

WMD—Weapons of Mass Destruction

Terms

Active Defense—The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.

Air Force Emergency Management (EM) Program—The single, integrated Air Force program to coordinate and organize efforts to prepare for, prevent, respond to, recover from and mitigate the direct and indirect consequences of an emergency or attack. The primary missions of the Air Force EM program are to (1) save lives, (2) minimize the loss or degradation of resources and (3) continue, sustain and restore combat and combat support operational capability in an all-hazards physical threat environment at Air Force installations worldwide. The ancillary missions of the Air Force EM program are to support homeland defense and civil support operations and to provide support to civil and host nation authorities IAW DOD directives and through the appropriate Combatant Command. The Air Force EM program is managed by the Office of The Civil Engineer, AF/A7C.

Antiterrorism (AT)—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

Assessment—Analysis of the security, effectiveness and potential of an existing or planned intelligence activity. (JP 1-02) [The evaluation of progress toward the creation of effects and the achievement of objectives and end state conditions.][AFDD 2-1.9]{Words in brackets apply only to the Air Force and are offered for clarity.}

AT Awareness—Fundamental knowledge of both the terrorist threat and the measures to reduce personal vulnerability to terrorism.

AT Officer (ATO)—The principal military or civilian advisor charged with managing the AT program for the commander or DOD civilian exercising equivalent authority.

AT Planning—The process of developing specific guidance and execution-oriented instructions for subordinates. An AT plan contains command-specific guidance for the establishment of an AT program and the implementation of the AT Standards.

AT Program—One of several security-related programs that fall under the overarching combating terrorism and FP programs. The AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DOD personnel and their families, facilities, installations and infrastructure critical to mission accomplishment as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource application and a program review.

AT Program Review—The process of developing specific guidelines used to evaluate the AT Program in order to assess satisfactorily and evaluate the effectiveness and adequacy of the AT Program.

AT Resource Application—The process of applying risk management to vulnerabilities and where the resultant risk is not acceptable after applying mitigation measures, elevate the vulnerability with a resource request using the existing PPB&E system, the CbT-RIF, the Physical Security Program and other funding mechanisms. Central to success in resource application is tracking and ensuring sufficient funding for identified AT program life-cycle costs and assessed shortfalls to mitigate risk associated with terrorist capabilities.

AT Risk Management—The process of systematically identifying, assessing and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits. The end products of the AT program risk management process shall be the identification of DOD elements and personnel that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT risk management (threat assessment, criticality assessment and vulnerability assessment), the commander must determine which DOD elements and personnel are at greatest risk and how best to employ given resources and FP measures to deter, mitigate or prepare for a terrorist incident.

AT Training and Exercises—The process of developing individual, leader and collective skills and of conducting comprehensive exercises to validate plans for AT incident response, consequence management and continuity of essential military operations.

Biological Select Agents and Toxins (BSAT)—Biological agents and toxins that present a high bioterrorism risk to national security and have the greatest potential for adverse public health impact with mass casualties of humans and/or animals or that pose a severe threat to plant health or to plant products. The lists are reviewed and updated by HHS/CDC and USDA/APHIS. Agents and toxins that are excluded in Title 42, Code of Federal Regulations, Part 73, and Title 7, Code of Federal Regulations, Part 331 are excluded as BSAT.

Combating Terrorism (CbT)—For the purposes of this Instruction, combating terrorism within the DOD encompasses all actions, including AT, counterterrorism, terrorism consequence management (preparation for and response to the consequences of a terrorist incident or event) and terrorism intelligence support (collection and dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum, including terrorist use of CBRNE.

Combating Terrorism Readiness Initiatives Fund (CbT-RIF)—Program established by Congress in the FY 1997 National Defense Authorization Act and managed by the J-3 DDAT/HD. Provides funds for emergency and emergent high-priority antiterrorism projects or equipment submitted by combatant commands and approved by the Chairman of the Joint Chiefs of Staff or a designated representative, after coordination with the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and the Services.

Commander—Personnel assigned to command positions at all levels and the heads of the Defense Agencies and DOD Field Activities.

Commander's Critical Information Requirements (CCIR)—An information requirement identified by the commander as being critical to facilitating timely decision-making. The two key elements are friendly force information requirements and priority intelligence requirements.

Comprehensive AT Program Review—The systematic assessment of the AT program against the AT Standards.

Consequence Management—For the purpose of this Instruction, consequence management is those measures taken to protect public health and safety, restore essential Government services and provide emergency relief to governments, businesses and individuals affected by the consequences of a CBRNE situation. For domestic consequence management, the primary authority rests with the States to respond. The Federal Government responds through the Department of Homeland Security's Federal Emergency Management Agency, as the Lead Federal Agency (LFA) for providing assistance as required. DOS is the LFA for foreign consequence management.

Coordination—The necessary action to ensure adequate exchange of information to integrate, synchronize and deconflict operations between separate organizations. Coordination is not necessarily a process of gaining approval but is most often used for mutual exchange of information. Normally used between functions of a supporting staff. Direct liaison authorized (DIRLAUTH) is used to coordinate with an organization outside of the immediate staff or organization.

Counterintelligence (CI)—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or persons, or international terrorist activities.

Criminal Intelligence (CRIMINT)—Law enforcement information derived from the analysis of information collected through investigations, forensics, crime scene and evidentiary processes to establish intent, history, capability, vulnerability and modus operandi of threat and criminal elements.

Crisis Management—For the purpose of this Instruction, crisis management is those measures taken to resolve a hostile situation and to investigate and prepare a criminal case for prosecution under Federal law. Crisis management shall include a response to an incident involving WMD, a special improvised explosive device or a hostage crisis that is beyond the capability of the LFA.

Critical Asset—An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DOD Components or Defense Infrastructure Sector Lead Agents to execute the task or MET it supports. TCAs are used to identify defense critical assets.

Criticality Assessment—For the purposes of this Instruction, an assessment of the effect of temporary or permanent loss of key assets or infrastructures on the installation or a unit's ability to perform its mission. The assessment also examines costs of recovery and reconstitution including time, funds, capability and infrastructure support.

Defense Critical Asset—An asset of such extraordinary importance to DOD operations in peace, crisis and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its mission.

Defense Critical Infrastructure (DCI)—Department of Defense and non-Department of Defense networked assets and essential to project, support and sustain military forces and operations worldwide.

Deterrence—The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.

DOD AT Program—The minimum elements of the DOD AT program as a whole and of DOD Component AT programs are AT risk management, planning, training and exercises, resource application and program review.

DOD Civilian Work Force—U.S. citizens or foreign nationals working for the Department of Defense and paid from appropriated or non-appropriated funds under permanent or temporary appointment. This includes employees filling full-time, part-time, intermittent or on-call positions. Specifically excluded are all Government contractor employees.

DOD Component—The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense Agencies, field activities and all other organizational entities in the Department of Defense.

DOD Contractor—Any individual, firm, corporation, partnership, association or other legal non-Federal entity that enters into a contract directly with the Department of Defense to furnish services, supplies or both, including construction. Defense contractors may include U.S. nationals, local citizens or third country nationals. Defense contractors do not include foreign governments or representatives of foreign governments that are engaged in selling to the Department of Defense or a DOD Component or foreign corporations wholly owned by foreign governments.

DOD Elements and Personnel—For the purposes of this Instruction, DOD military and civilian personnel and their dependent family members; DOD contractors; DOD installations and facilities; DOD-owned, -leased or -managed defense critical infrastructure.

DOD Personnel—For the purposes of this Instruction, Uniformed Military Service members and DOD Federal civilian employees hired and paid from appropriated and non-appropriated funds under permanent or temporary appointment.

Eagle Eyes Program—A CSAF-approved Air Force antiterrorism defensive program created to enhance the collection of threat information by educating members of the Total Force and off-base citizens on the nature of terrorist attack-planning activities. The program also establishes 24-hour phone numbers to call when suspicious behavior is observed.

Emergency CbT-RIF Requirement—An unanticipated CbT-RIF requirement created by a combination of circumstances or the resulting state that requires IMMEDIATE action to prevent, deter or respond to a terrorist act.

Emergency Responders—Firefighters, law enforcement, security personnel, emergency medical technicians, emergency management and operations personnel, explosive ordnance disposal personnel, physicians, nurses, medical treatment providers at medical treatment facilities, disaster preparedness officers, public health officers, bioenvironmental engineers, counterintelligence agents and mortuary affairs personnel.

Emergent CbT-RIF Requirement—A newly-formed unexpected CbT-RIF requirement resulting as a logical consequence of unforeseen circumstances and calling for PROMPT action.

Facility—A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement and underlying land.

Family Member—Individuals defined as “Dependent” in section 1072(2) of title 10 U.S.C.

First Responder—Firefighters, law enforcement and/or security personnel, emergency medical technicians and EOD personnel (for suspected explosive CBRNE events) that provide the initial, immediate response to an accident, disaster, criminal, terrorist or CBRNE incident.

Food and Water Security—The protection of food and water sources from disruption and contamination or other terrorist acts that could severely impact operations. Food and water security measures include those actions taken to detect, prevent and mitigate the effects from intentional acts designed to disrupt or contaminate food and water sources.

Force Health Protection (FHP)—A comprehensive threat-based program directed at preventing and managing health related actions against Air Force uncommitted combat power.

Force Protection (FP)—Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities and critical information. These actions conserve the force’s fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather or disease. (JP 1-02) [An integrated application of offensive and defensive actions that deter, detect, preempt, mitigate or negate threats against or hazards to Air Force air and space operations and assets, based on an acceptable level of risk.]{Definition in brackets applies only to the Air Force and is offered for clarity.}

Force Protection Condition (FPCON)—A DOD-approved system standardizing the Department’s identification, recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. This system is the principal means for a commander to apply an operational decision on how to protect against terrorism. It facilitates inter-Service coordination and support for AT activities.

Force Protection Detachment (FPD)—A CI element that provides comprehensive CI support to transiting ships, personnel and/or aircraft in regions of elevated threat.

Force Protection Intelligence (FPI)—Analyzed, all-source information concerning threats to DOD missions, people or resources arising from terrorists, criminal entities, foreign intelligence and security services and opposing military forces. FPI supports FP decisions and operations

Foreign Intelligence—Information relating to capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence, except for information on international terrorist activities. See also intelligence.

High-Risk Billet (HRB)—Authorized personnel billet (designated by the appropriate authority as identified in DODI O-2000.22) that because of grade (normally, General, Admiral or Senior Executive Service equivalent and assigned in a country with a DIA terrorist threat level of "Significant" or higher), assignment, travel itinerary or symbolic value may make a person filling it an especially attractive or accessible terrorist target.

High-Risk Personnel (HRP)—Personnel who, by their grade, assignment, symbolic value or relative isolation, are likely to be attractive or accessible terrorist targets.

Higher Headquarters Assessment (HHA)—An overall assessment by a higher headquarters of how an organization is managing its AT program, including management and compliance efforts by subordinate organizations.

Installation—A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base.

Installation Commander—The individual responsible for all operations performed by an installation.

Intelligence—The product resulting from the collection, processing, integration, evaluation, analysis and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. See also acoustic intelligence; all-source intelligence; basic intelligence; civil defense intelligence; combat intelligence; communications intelligence; critical intelligence; current intelligence; departmental intelligence; domestic intelligence; electronic intelligence; electro-optical intelligence; foreign intelligence; foreign instrumentation signals intelligence; general military intelligence; human resources intelligence; imagery intelligence; joint intelligence; laser intelligence; measurement and signature intelligence; medical intelligence; merchant intelligence; military intelligence; national intelligence; nuclear intelligence; open-source intelligence; operational intelligence; photographic intelligence; political intelligence; radar intelligence; radiation intelligence; scientific and technical intelligence; security intelligence; strategic intelligence; tactical intelligence; target intelligence; technical intelligence; technical operational intelligence; terrain intelligence; unintentional radiation intelligence.

Joint Staff Integrated Vulnerability Assessment (JSIVA)—A vulnerability-based evaluation of an installation's ability to deter and/or respond to a terrorist incident. A vulnerability-based assessment considers both the current threat and the capabilities that may be employed by both transnational and local terrorist organizations, both in terms of their mobility and the types of weapons historically employed.

Mutual Aid Agreement—Written agreement between agencies, organizations, or jurisdictions that they will assist one another on request by furnishing personnel, equipment, or expertise in a specified manner. Reciprocal assistance by local government and an installation for emergency services under a prearranged plan. Mutual aid is synonymous with "mutual assistance," "outside aid," "memorandums of understanding," "memorandums of agreement," "letters of agreement," "cooperative assistant agreement," "intergovernmental compacts," or other similar agreements, written or verbal, that constitute an agreed reciprocal assistance plan for sharing emergency services. MAAs between entities are an effective means to obtain resources and should be developed whenever possible. MAAs should be in writing, be reviewed by legal counsel and be signed by a responsible official.

Physical Security—For the purposes of this Instruction, that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage and theft.

Priority Intelligence Requirement (PIR)—Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision-making.

Protection Providing Organization (PPO)—Refers collectively to the U.S. Army Criminal Investigation Command, the Naval Criminal Investigative Service, Air Force Office of Special Investigations, the Defense Criminal Investigative Service, the Pentagon Force Protection Agency and the National Security Agency.

Protective Services—A specialized activity, which increases the personal safety and security of a distinguished visitor or other principal. The activity may be limited to a protective threat assessment or may extend to a major PSO involving considerable manpower and resources.

Protective Service Detail (PSD)—Trained and armed protective security officials capable of providing continuous protection for a designated individual.

RED HORSE—Air Force units are wartime-structured to provide a heavy engineer capability. They have a responsibility across the operational area, are not tied to a specific base, and are not responsible for base operation and maintenance. These units are mobile, rapidly deployable, and largely self-sufficient, for limited periods of time.

Security—For the purposes of this Instruction, measures taken by a military unit, activity, or installation to protect against all acts designed to, or that may, impair its effectiveness. Also, a condition that results from establishing and maintaining protective measures that ensures a state of inviolability from hostile acts or influences.

Self-Supported Separate Facility—A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement and underlying land that is separate from an installation and has inherent responsibility for emergency response functions, e.g. 911 response functions.

Special Event—An activity characterized by a large concentration of personnel and/or a gathering where distinguished visitors are involved, often associated with a unique or symbolic event.

TACON for FP—TACON that enables the GCC to order implementation of FP measures and to exercise the security responsibilities outlined in any MOA concluded pursuant to MOU between

DOS and DOD, "Security of DOD Elements and Personnel in Foreign Areas," (known as the Universal MOU). Further, TACON for FP authorizes the GCC to change, modify, prescribe and enforce FP measures for covered forces. This relationship includes the authority to inspect and assess security requirements, direct DOD activities to identify the resources required to correct deficiencies and submit budget requests to parent organizations to fund identified corrections. The GCC may also direct immediate FP measures (including temporary relocation and departure) when in his or her judgment such measures must be accomplished without delay to ensure the safety of the DOD personnel involved. Persons subject to TACON for FP of a GCC include Active and Reserve Component personnel (including National Guard personnel in a title 10 status (Sections 134 and 1072(2) of title 10, USC)) in the AOR as well as all DOD civilian employees and their family members in the AOR.

Terrorism—The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. See also antiterrorism; combating terrorism; counterterrorism; force protection condition; terrorist; terrorist groups.

Terrorism Consequence Management—DOD preparedness and response for mitigating the consequences of a terrorist incident, including the terrorist use of WMD. DOD consequence management activities are designed to support the lead Federal agency (domestically, the Department of Homeland Security; foreign, the Department of State) and include measures to alleviate damage, loss of life, hardship, or suffering caused by the incident; protect public health and safety; and restore emergency essential government services.

Terrorism Incident Response Measures—A set of procedures established for response forces to deal with the effects of a terrorist incident.

Terrorism Threat Assessment—The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat or the product of a threat analysis for a particular unit, installation, or activity.

Terrorism Threat Level (TTL)—An intelligence threat assessment of the level of terrorist threat faced by U.S. personnel and interests. The assessment is based on a continuous intelligence analysis of a minimum of four elements: terrorist group operational capability, intentions, activity and operational environment. There are four threat levels: LOW, MODERATE, SIGNIFICANT and HIGH. Threat levels should not be confused with FPCONs. Threat-level assessments are provided to senior leaders to assist them determining the appropriate local FPCON.

Terrorist—An individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives.

Terrorist Groups—Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatens violence in pursuit of their political, religious, or ideological objectives. See also terrorism.

Unit—1. Any military element whose structure is prescribed by competent authority, such as a table of organization and equipment; specifically, part of an organization. 2. An organization title of a subdivision of a group in a task force. 3. With regard to Reserve Components of the

Armed Forces, denotes a Selected Reserve unit organized, equipped and trained for mobilization to serve on active duty as a unit or to augment or be augmented by another unit.

Unit Antiterrorism Representative—The principal military or civilian advisor charged with managing the AT program for a unit or DOD element not required to have an ATO as stipulated in AF AT Standard 9.

Vulnerability—In AT, a situation or circumstance which, if left unchanged, may result in the loss of life or damage to mission-essential resources. It includes the characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

Vulnerability Assessment (VA)—A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism.

Weapons Of Mass Destruction (WMD)—Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high-yield explosives or nuclear, biological, chemical, or radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

Attachment 2

FORCE PROTECTION CONDITION (FPCON) MEASURES

A2.1. General. The DOD FPCON System describes the progressive level of protective measures that are implemented by all the DOD Components in anticipation of or in response to a terrorist threat or attack. The FPCON System is the principal means through which commanders apply an operational decision on how to best guard against the terrorist threat. The protective measures identified in the FPCON System assist commanders in reducing the risks of terrorist attacks and other security threats to DOD personnel, units and activities. The measures below are derived from DOD AT Standard 22 and include AF modifications. Commanders will ensure these measures and developed measures address local and operational risks. Commanders must consider GCC policies, local laws, mutual support agreements and/or the SOFA. Air Force commanders are responsible for implementing FPCON measures.

A2.1.1. Commanders shall ensure the following when implementing FPCON measures:

A2.1.1.1. Ensure there is an effective AT plan and the plan is widely known and practiced in order to use “every airman as a sensor”.

A2.1.1.2. Analyze the threat and plan courses of action to defeat those threats. Detailed planning against plausible enemy courses of action will often point to vulnerabilities which can be mitigated through adjustments to TTPs and further mitigated through innovation and programming.

A2.1.1.3. Consider force on force or intruder play to test COAs. Development and implementation of effective friendly COAs to counter known threats offers a reasonable deterrent effect and the opportunity for long-term success against terrorist attack.

A2.1.1.4. Ensure personnel assigned tasks directed by FPCON measures are properly trained and available to carry out the task.

A2.1.1.5. Based on the threat, employ sufficient patrols to deter enemy action, disrupt terrorist planning and respond to incidents or attacks against the installation. Patrols should focus protection on critical operational assets, mission support infrastructure and mass gathering locations.

A2.1.1.6. Consider placing barriers around identified critical assets, facilities with BSAT, restricted areas, high occupancy facilities, flight line entry points and high value resource areas to create standoff.

A2.1.1.7. Review and be familiar with mutual aid and host tenant support agreements. Keep law enforcement agencies (federal, state and local) appraised of the current situation and threat to determine the level of incident support the installation provides or receives.

A2.1.1.8. Ensure the installation Disaster Response Force and its sub elements are trained and available for response as described in AFI 10-2501.

A2.1.2. The DOD FPCON System consists of five progressive levels of increasing AT protective measures.

A2.1.3. Site-specific AT measures and physical security actions, linked to an FPCON, shall be classified “CONFIDENTIAL.” When separated from the AT Plan, specific AT measures linked to a FPCON and site-specific FPCON levels may be downgraded to “FOR OFFICIAL USE ONLY,” if appropriate.

A2.1.4. Upon declaration of an FPCON level, all listed security measures for that FPCON level shall be implemented immediately unless waived in writing by the appropriate GCC or delegated representative. In non-DOD controlled facilities housing DOD occupants, DOD organizations shall implement applicable FPCON measures in space directly controlled by DOD to the extent possible. The supplementing RAMs and command-unique or site-specific measures should also be implemented to complicate a terrorist group’s operational planning and targeting.

A2.1.5. AF installations and separate facilities shall supplement each FPCON measure in this instruction with site-specific details describing how the measure is to be implemented locally, to include responsibilities assigned to subordinate units and organizations.

A2.1.6. Airfield-specific measures are for installations and facilities with a permanently functioning airfield. Installations and facilities with an emergency helicopter pad should review and implement any applicable airfield-specific measures when they anticipate air operations.

A2.1.7. The CBRN related FPCON measures contained in this publication are not all inclusive. Additional CBRN FPCON measures are in the AF Civil Engineer Support Agency (AFCESA) Comprehensive Emergency Management Plan (CEMP) 10-2 template. Each MAJCOM and installation should also develop additional CBRN FPCON measures applicable to their location.

A2.2. FPCON NORMAL. This condition applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DOD installations and facilities.

A2.2.1. Measure NORMAL 1: Secure and randomly inspect buildings, rooms and storage areas not in regular use.

A2.2.2. Measure NORMAL 2 (AF Modified): Conduct random security checks of vehicles and persons entering facilities under the jurisdiction of the United States.

A2.2.2.1. Measure NORMAL 2.1 (AF Added): Conduct random vehicle inspections at installation entry points in addition to base entry point checks (BEPC) as directed by installation commanders. Implement 100% inspection of large commercial vehicles. MAJCOM and local planners should define large commercial vehicles in integrated defense plans based on geographical location, character of local transport and threat. Conduct random vehicle inspections at entrances to restricted areas beyond inspection requirements listed in AFI 31-101.

A2.2.3. Measure NORMAL 3: Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

A2.2.4. Measure NORMAL 4 (AF Modified): Identify defense critical infrastructure and critical assets, facilities with BSAT and high occupancy buildings.

A2.2.5. Measure NORMAL 5 (AF Added): Implement a daily RAM program involving the entire installation with emphasis on identifying surveillance activities and disrupting the terrorist attack cycle. Installations will tailor their RAM program to meet the threat and mitigate vulnerabilities.

A2.2.6. Measure NORMAL 6 (AF Added): Conduct 100% identification verification of all vehicle operators and pedestrians entering installations.

A2.2.7. Measure NORMAL 7 (AF Added): Where no permanent channeling measures are built into the gates, emplace barriers or obstacles on in-bound and out-bound lanes at installation entry points to mitigate high-speed installation access through entry and exit lanes, in accordance with UFC 4-022-01. Prevent base entry through exit lanes. Ensure sufficient number and types of barriers remain for increased FPCON/RAMs.

A2.2.8. Measure NORMAL 8 (AF Added): Identify local vendors that are able to provide rapid stocks of emergency response equipment and supplies in accordance with local response plans.

A2.3. FPCON ALPHA. (AF Modified) This condition applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. However, it may be necessary to implement certain measures from higher FPCONs measures resulting from intelligence received or as a deterrent. The measures in this FPCON must be capable of being maintained indefinitely.

A2.3.1. Measure ALPHA 1: Fully implement all measures of lower FPCON levels.

A2.3.2. Measure ALPHA 2: At regular intervals, inform personnel and family members of the general situation. Ensure personnel arriving for duty are briefed on the threat. Also, remind them to be alert for and to report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels and possible surveillance attempts.

A2.3.2.1. Measure ALPHA 2.1 (AF Added): Post signs at installation gates and utilize mass communication systems to inform/remind personnel of the FPCON level.

A2.3.3. Measure ALPHA 3: The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Plans should be in place to execute access control procedures. Key personnel required to implement security plans should be on-call and readily available.

A2.3.4. Measure ALPHA 4 (AF Modified): Increase random security checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States.

A2.3.5. Measure ALPHA 5: Initiate food and water risk management procedures, brief personnel on food and water security procedures and report any unusual activities.

A2.3.6. Measure ALPHA 6 (AF Modified): Test mass notification systems weekly.

A2.3.7. Measure ALPHA 7: Review all plans, identify resource requirements and be prepared to implement measures of the next higher FPCON level.

A2.3.7.1. Measure ALPHA 7.1 (AF added): Review plans (to include AT, Comprehensive Emergency Management Plan, Integrated Defense Plan, Medical Contingency Response Plan/Mass Casualty, Disease Containment Plan, etc.) and most recent VA reports, and identify resource requirements. Review dependent, civilian and military personnel evacuation plans and support agreements with local officials.

A2.3.8. Measure ALPHA 8 (AF Modified): Review and, if necessary, implement security measures for DOD identified high-risk personnel in accordance with DODI O-2000.22 and AFI 71-101, vol 2, *Protective Service Matters*.

A2.3.9. Measure ALPHA 9 (AF Modified): Consult local authorities on the threat and mutual AT measures. As appropriate, brief law enforcement agencies who provide support to the installation and request assistance as necessary to ensure protection of resources and personnel.

A2.3.10. Measure ALPHA 10: Review intelligence, CI and operations dissemination procedures.

A2.3.11. Measure ALPHA 11: Review barrier plans.

A2.3.12. Measure ALPHA 12 (AF Added): Secure access to all bulk quantity storage areas containing hazardous and flammable material.

A2.3.13. Measure ALPHA 13 (AF Added): Review CBRN detection plan ensuring it uses available detectors (deployment and home station assets).

A2.3.14. Measure ALPHA 14: Review all higher FPCON measures.

A2.4. FPCON BRAVO. Applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and military-civil relationships with local authorities.

A2.4.1. Measure BRAVO 1: Fully implement all measures of lower FPCON levels.

A2.4.1.1. Measure BRAVO 1.1 (AF Added): Brief personnel on the updated threat and associated procedures. Update signs at installation gates and utilize mass communication systems to inform/remind personnel of the FPCON level.

A2.4.1.2. Measure BRAVO 1.2 (AF Added): Increase frequency of daily RAMs. Focus additional RAMs on current situation and nature of threat.

A2.4.1.3. Measure BRAVO 1.3 (AF Added): Have intelligence and OSI provide a CBRN threat briefing to the Threat Working Group (TWG) or equivalent. Include specific information such as probability of CBRN use, type(s) and amount of CBRN material, likely CBRN material release mechanisms and probable targets.

A2.4.1.4. Measure BRAVO 1.4 (AF Added): Verify the interoperability of CBRN response procedures with local community resources, to include activities outlined in the CEMP 10-2, Disease Containment Plan (DCP) and Medical Contingency Response Plan (MCRP).

A2.4.1.5. Measure BRAVO 1.5 (AF Added): Contact local hospitals and establish/ensure lines of communication for notification of the installation in the event of significant increase in antibiotic use or people exhibiting symptoms of exposure to CBRN materials.

A2.4.2. Measure BRAVO 2 (AF Modified): Enforce control of entry into facilities containing defense critical infrastructure and critical assets, BSAT, lucrative targets, or high-profile locations. Randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles that are capable of concealing a large improvised explosive device (IED), e.g., cargo vans or delivery vehicles, sufficient to cause catastrophic damage to property or loss of life.

A2.4.3. Measure BRAVO 3 (AF Modified): Keep cars and objects (e.g., crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all critical and high-occupancy buildings. Consider applying to all inhabited structures to the greatest extent possible. Standoff distance should be determined by the following factors: asset criticality, the protection level provided by structure, IED or Vehicle Borne IED (VBIED) threat and available security measures. Consider centralized parking and implementation of barrier plans. Utilize UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*, and UFC 4-010-02, *DOD Minimum Antiterrorism Standoff Distances for Buildings.* The AFH 10-2401, *Vehicle Bomb Mitigation Guide*, is an additional tool for standoff planning.

A2.4.4. Measure BRAVO 4: Secure and periodically inspect all buildings, rooms and storage areas not in regular use.

A2.4.5. Measure BRAVO 5: At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

A2.4.6. Measure BRAVO 6: Implement mail-screening procedures to identify suspicious letters and parcels.

A2.4.7. Measure BRAVO 7: Randomly inspect commercial deliveries. Advise family members to check home deliveries.

A2.4.7.1. Measure BRAVO 7.1 (AF Added): Increase random security checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States. Inspect all commercial deliveries (AF Baseline FPCON posture directs inspection of all large commercial vehicles in FPCON Normal).

A2.4.8. Measure BRAVO 8 (AF Modified): Randomly inspect food and water for evidence of tampering or contamination before use by DOD personnel. Inspections should include delivery vehicles, storage areas/facilities and storage containers.

A2.4.9. Measure BRAVO 9: Increase security measures and guard presence or initiate increased patrols and surveillance of DOD housing areas, schools, messes, on-base clubs, military treatment facilities and similar high-occupancy targets to improve deterrence and defense, and to build confidence among staff and family members.

A2.4.10. Measure BRAVO 10: Implement plans to enhance off-installation security for DOD facilities. In areas with Threat Levels of Moderate, Significant, or High, coverage includes facilities (e.g., DOD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DOD employees and family members.

A2.4.11. Measure BRAVO 11: Inform local security committees of actions being taken.

A2.4.11.1. Measure BRAVO 11.1 (AF Added): Consult local authorities on the threat and mutual AT measures. As appropriate, brief law enforcement agencies who provide support to the installation and request assistance as necessary to ensure protection of resources and personnel. As appropriate, coordinate with local authorities regarding infrastructure outside the installation, e.g. infrastructure supplying energy to the installation.

A2.4.12. Measure BRAVO 12 (AF Modified): Verify identity of visitors to the installation and randomly inspect their suitcases, parcels and other containers. Visitors are non-DOD affiliated personnel who do not have official DOD credentials authorizing installation access.

A2.4.13. Measure BRAVO 13: Conduct random patrols to check vehicles, people and buildings.

A2.4.14. Measure BRAVO 14: As necessary, implement additional security measures for High-Risk Personnel (HRP).

A2.4.15. Measure BRAVO 15: Place personnel required for implementing AT plans on call; commanders should exercise discretion in approving absences.

A2.4.16. Measure BRAVO 16: Identify and brief personnel who may augment guard forces. Review specific rules of engagement including the use of deadly force.

A2.4.17. Measure BRAVO 17: As deemed appropriate, verify identity of personnel entering buildings.

A2.4.18. Measure BRAVO 18: Review status and adjust as appropriate operations security, communications security and information security procedures.

A2.4.19. Measure BRAVO 19 (AF Modified): (Airfield-specific) Limit access points in order to enforce entry control. As appropriate, erect barriers and establish manned checkpoints at entrances to airfields. Ensure the identity of all individuals entering the airfield (flight line and support facilities) with no exceptions. Randomly inspect vehicles, briefcases and packages entering the airfield.

A2.4.20. Measure BRAVO 20: (Airfield-specific) Coordinate plans to safeguard aircraft departure and approach flight paths with local authorities. Be prepared to activate contingency plans and issue detailed air traffic control procedures. As appropriate, take actions to mitigate the threat of surface- to-air missiles or standoff weapons that can be delivered from beyond the airfield perimeter.

A2.4.21. Measure BRAVO 21 (AF Added): Ensure CBRN detectors are operational as outlined with the detection plan (deployment and home station assets).

A2.4.22. Measure BRAVO 22: Review all higher FPCON measures.

A2.5. FPCON CHARLIE. Applies when an incident occurs or intelligence is received indicating that some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.

A2.5.1. Measure CHARLIE 1: Fully implement all measures of lower FPCON levels.

A2.5.1.1. Measure CHARLIE 1.1 (AF Added): Conduct 100% identification checks of all personnel entering the installation, to include vehicle passengers.

A2.5.1.2. Measure CHARLIE 1.2 (AF Added): Brief personnel on the updated threat and associated procedures. Update signs at installation gates and utilize mass communication systems to inform/remind personnel of the FPCON level. If a CBRN threat exists, ensure the Disaster Response Force and, if permissible, local authorities are briefed on the threat.

A2.5.1.3. Measure CHARLIE 1.3 (AF Added): Increase frequency of daily RAMs. Focus additional RAMs on current situation and nature of threat.

A2.5.2. Measure CHARLIE 2: Recall additional required personnel. Ensure armed augmentation security personnel are aware of current rules of engagement and any applicable Status of Forces Agreements (SOFA). Review types of weapons and ammunition issued to augmentation security personnel; heightened threats may require employment of different weapon capabilities.

A2.5.3. Measure CHARLIE 3: Be prepared to react to requests for assistance from both local authorities and other installations in the region.

A2.5.3.1. Measure CHARLIE 3.1 (AF Added): Ensure flow of information between on and off-base medical treatment facilities participating in the medical surveillance program. Consider initiation of manual collection of data if the automated system has a 24-hour or more delay in providing results.

A2.5.3.2. Measure CHARLIE 3.2 (AF Added): Consider Noncombatant Evacuation Operations (NEO).

A2.5.4. Measure CHARLIE 4: Limit access points in order to enforce entry control. Randomly search vehicles.

A2.5.4.1. Measure CHARLIE 4.1 (AF Added): Increase random security checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States.

A2.5.4.2. Measure CHARLIE 4.2 (AF Added): Implement procedures to expedite the entry of first and emergency responders onto the installation during emergencies. Ensure these procedures prevent unauthorized entry.

A2.5.5. Measure CHARLIE 5: Ensure or verify the identity of all individuals entering food and water storage and distribution centers use sign-in and sign-out logs at access control and entry points, and limit or inspect all personal items.

A2.5.6. Measure CHARLIE 6 (AF Modified): Initiate contingency (credible CBRN threat) monitoring for chemical, biological and radiological contamination as required. Suspend contractors and off-facility users from tapping into the facility water system. An alternate locally developed measure should be implemented when contractors are responsible for DOD water supplies or when water is provided by local (non-DOD) sources or agencies.

A2.5.6.1. Measure CHARLIE 6.1 (AF Added): If a CBRN threat exists, ensure all shortages of CBRN equipment and its potential impact is briefed to the installation commander.

A2.5.6.2. Measure CHARLIE 6.2 (AF Added): Verify operation, deploy and begin using all available CBRN detectors (deployment and home station) as outlined in the detection plan.

A2.5.7. Measure CHARLIE 7: Increase standoff from sensitive buildings based on the threat. Implement barrier plan to hinder vehicle-borne attack.

A2.5.8. Measure CHARLIE 8 (AF Modified): Increase patrolling of the installation/facility to include waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threatening actions/persons outside the facility perimeter. For airfields, patrol or provide observation of aircraft parking areas and approach and departure flight corridors as appropriate to the threat (coordinate with Transportation Security Administration, Marine Patrol, United States Coast Guard and local law enforcement as required to cover off-facility approach and departure flight corridors).

A2.5.9. Measure CHARLIE 9 (AF Modified): Increase protection for all defense critical infrastructure, critical assets or BSAT facilities. Give special attention to and coordinate with local authorities regarding infrastructure outside the military establishment.

A2.5.9.1. Measure CHARLIE 9.1 (AF Added): Consider closing or enhancing security at remote sites and alternate, practice or training airfields.

A2.5.9.2. Measure CHARLIE 9.2 (AF Added): Protect DOD personnel at vulnerable mass gathering facilities during peak usage, especially near the installation perimeter. Coordinate protection of mass gathering facilities off the installation with civilian law enforcement agencies.

A2.5.10. Measure CHARLIE 10: To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter.

A2.5.11. Measure CHARLIE 11: Randomly inspect suitcases, briefcases and packages being brought onto the installation through access control points and consider randomly searching them upon leaving the installation.

A2.5.12. Measure CHARLIE 12: Review personnel policy procedures to determine appropriate courses of action for dependent family members.

A2.5.13. Measure CHARLIE 13: Review access procedures for all non-U.S. personnel and adjust as appropriate. For airfields, consider terminating visitor access to the flight line and support facilities.

A2.5.14. Measure CHARLIE 14: Consider escorting children to and from DOD schools (among options to consider are escorting school buses, recommending parents escort children to/from school, etc.).

A2.5.15. Measure CHARLIE 15: (Airfield-specific) Reduce flying to only essential operational flights. Implement appropriate flying countermeasures as directed by the Flight Wing Commander (military aircraft) or Transportation Security Administration (civilian aircraft). Consider relief landing ground actions to take for aircraft diversions into and out of an attacked airfield. Consider augmenting fire-fighting details.

A2.5.15.1. Measure CHARLIE 15.1 (AF Added): Consider aircraft dispersal, or the dispersal of other high value assets, based on assessment of local threat from standoff weapons, vulnerability of the assets and operational feasibility.

A2.5.16. Measure CHARLIE 16: Review all FPCON DELTA measures.

A2.6. FPCON DELTA. Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. FPCON DELTA is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration.

A2.6.1. Measure DELTA 1 (AF Modified): Fully implement all measures of lower FPCON levels. As necessary, brief personnel on the updated threat and associated procedures and update signs at installation gates, utilize mass communication systems to inform/remind personnel of the FPCON level.

A2.6.2. Measure DELTA 2: Augment guards as necessary.

A2.6.3. Measure DELTA 3: Identify all vehicles within operational or mission support areas.

A2.6.4. Measure DELTA 4: Search all vehicles and their contents before allowing entrance to the installation. Selected pre-screened and constantly secured vehicles used to transport escorted very important personnel may be exempted.

A2.6.5. Measure DELTA 5: Control facility access and implement positive identification of all personnel with no exceptions.

A2.6.6. Measure DELTA 6: Search all personally carried items (e.g., suitcases, briefcases, packages, backpacks) brought into the installation or facility.

A2.6.7. Measure DELTA 7: Close DOD schools.

A2.6.8. Measure DELTA 8: Make frequent checks of the exterior of buildings and of parking areas.

A2.6.9. Measure DELTA 9: Restrict all non-essential movement.

A2.6.10. Measure DELTA 10: (Airfield specific) Cease all flying except for specifically authorized operational sorties. Be prepared to deploy light aircraft and/or helicopters for surveillance tasks or to move internal security forces. Implement, if necessary, appropriate flying countermeasures.

A2.6.11. Measure DELTA 11: (Airfield specific) As appropriate, airfields should prepare to accept aircraft diverted from other stations.

A2.6.12. Measure DELTA 12: If permitted, close public and military roads and facilities. If applicable, close military roads allowing access to the airfield.

A2.6.13. Measure DELTA 13: Begin continuous monitoring for chemical, biological and radiological contamination.

A2.6.14. Measure DELTA 14 (AF Added): If not already accomplished and a credible threat exists, initiate collective protection operations, as explained in AFMAN 10-2602, *Nuclear, Biological, Chemical, and Conventional (NBCC) Defense Operations and Standards*.

Attachment 3

TERRORIST THREAT LEVELS

A3.1. General. The standardized DOD methodology that describes the terrorist threat to DOD personnel, facilities and interests shall be used to determine Terrorism Threat Levels (TTL). The Defense Intelligence Agency (DIA) sets the DOD TTL for all countries. Terrorism threat levels are established as the result of all-source analysis and incorporation of GCC and Military Department input. The JITF-CT coordinates country TTLs with appropriate GCCs, Services and Defense Attaches.

A3.1.1. DIA and the responsible GCC may assign different threat levels to the same country. This is possible because analysts occasionally disagree about the conclusions to be drawn from available information. Threat assessments provide information to assist commanders in determining the appropriate FPCON level and measures. FPCON level declarations remain the exclusive responsibility of commanders. Threat levels are not tied to FPCON levels in any way and should not be confused. National-level DOD organizations cannot provide all intelligence that might be needed to make FPCON level determinations. Information from regional and tactical intelligence and local law enforcement authorities must also be considered.

A3.1.2. Threat assessments are not to be confused with DOD-designated high physical threat countries. DOD-designated high physical threat countries pertain exclusively to the DOD Travel Security Policy.

A3.2. Terrorist Threat Levels. In assessing the terrorist threat to U.S. personnel and interests, DOD intelligence agencies use a four-step scale to describe the severity of the threat. The following lists the threat levels and the combinations of analysis-based factors used to determine the level:

A3.2.1. **HIGH:** Anti-US terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. There is a substantial DOD presence and the operating environment favors the terrorist.

A3.2.2. **SIGNIFICANT:** Anti-US terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty producing attacks as their preferred method, but has limited operational activity. The operating environment is neutral.

A3.2.3. **MODERATE:** Terrorists are present, but there are no indications of anti-US activity. The operating environment favors the Host Nation/US.

A3.2.4. **LOW:** No group is detected or the group activity is non-threatening.

A3.3. Terrorist threat levels are a product of the following four factors.

A3.3.1. **Operational Capability**. This factor focuses on the attack methods used by the group and other measures that enhance its effectiveness, such as state sponsorship and ingenious use of technology. The key element is whether the group has the capability and willingness to conduct large casualty producing attacks, for example a suicide vehicle bomb containing thousand of kilograms of explosives or WMD timed to kill the most personnel at the target. Groups that selectively assassinate individuals or conduct late night bombings causing limited property damage pose a decreasing threat. The ability to operate on a regional or transnational basis and the overall professionalism of the group is also assessed.

A3.3.2. **Intentions**. This factor is the stated desire or history of terrorist attacks against U.S. interests. Recent substantial attacks in the country or, if the group is transnational, the conduct of operations in other countries is the higher end of the threat scale. This is especially true if the intentions are anti-DOD. The basis of the group ideology, whether the group is more focused on the host nation rather than U.S. interests is the other key component. Whether the group will react to high profile U.S. led international events, such as intervention in the Balkans, is also considered and rated.

A3.3.3. **Activity**. This factor is an assessment of the actions the group is conducting and whether that activity is focused on serious preparations for an attack. The highest threat is credible indications of U.S. targeting to include the movement of key operatives, final intelligence collection and movement of weapons to the target vicinity. Less threatening actions are contingency planning, training and logistical support. Activities that would make the group less likely to attack, such as robust fund raising or effective safe haven are considered. Whether the group has recently been disrupted by arrests or strikes on training camps will reduce the threat, at least in the short term.

A3.3.4. **Operating Environment**. This factor rates how the overall environment influences the ability, opportunity and motivation to attack DOD interests in a given location. An important element of this factor is the capability of the host nation security apparatus to combat terrorism, its degree of cooperation with the U.S. and the quality of the reporting on terrorist groups in the country. A key element is whether there is a DOD presence and if so the type, size, location, political sensitivity and if temporary, its duration. It is also important to consider if the group is focused on DOD as its primary target for anti-US attacks. Another part of this factor is the overall political, economic and military stability of the country and its effect on the ability of a group to attack.

Attachment 4

RISK MANAGEMENT AND RESOURCING PROCESSES

A4.1. Overview. The commander has an inherent command responsibility to reduce risks that threaten the mission with available resources. Risk management described in AFPD 31-1, aids the commander in assessing risk. If the commander cannot internally correct, mitigate or assume risk, they must elevate these vulnerabilities and associated risk(s) through CVAMP. CVAMP will forward the vulnerability through the chain of command to the GCC, who will decide if the vulnerability will be reported higher.

A4.2. Resourcing. Emphasis should be placed on acquiring resources to detect, assess, warn, defend or recover in order to prevent hostile acts or mitigate the effects. It is inherent upon the organization to assess the resource requirement against other organizational unfunded or funded requirements and determine if an internal reallocation of funding is appropriate and possible. CVAMP is used to collate and track AT vulnerabilities and resourcing. The status of vulnerabilities entered into CVAMP should be documented in CVAMP.

A4.3. AF Funding Sources.

A4.3.1. Planning, Programming, Budget and Execution (PPB&E). The PPB&E process includes requests considered during the POM funding cycle. This program is for long term planning and the funds will not be available for two to five years. Information on the PPB&E process can be found in the DOD Management Initiative Decision 913.

A4.3.2. Installation and MAJCOM budget process and commander's discretionary funds.

A4.3.3. Many PEC and/or funding appropriations (AT, Physical Security, EM, Medical, Construction, Base Defense, Base Operating Support, Communications, Weapons of Mass Destruction Threat Response; Nuclear, Biological and Chemical Defense Program; Fire Emergency Services; Sustainment Restoration and Modernization (SRM) and military construction (MILCON), etc.) may be used to fund AT resourcing activities. Commanders will consider all PEC and Funding Appropriation sources as authorized by law and AF policy and guidance.

A4.3.4. Use Antiterrorism Program Element 28047F as the primary funding source for manpower authorizations, antiterrorism equipment, procurement, military construction and the associated costs specifically identified and measurable to those resources and activities associated with the Air Force AT Program.

A4.3.4. **(ACC)** AT funds (PEC 28047) will be dispersed to primarily mitigate or correct vulnerabilities/concerns identified during VA's and loaded in CVAMP. CVAMP UFR submissions will be the primary source for funding data calls. CVAMP administrators shall ensure UFRs are correctly inputted, monitored, and updated at least quarterly.

A4.3.5. Specialized funds designed for AT and the war on terrorism.

A4.4. Combating Terrorism Readiness Initiative Fund (CbT-RIF). This program was established by Congress and is managed by the Joint Staff (J-3). It provides funds for emergency or unforeseen (emergent) high priority force protection projects or equipment. It is designed for requirements that need to be funded in the current fiscal year and provides a means for the GCC to react to unforeseen requirements from changes in a terrorist threat, threat levels, force protection doctrine/standards, as well as unanticipated requirements identified as a result of VAs, tactical operations and exercising AT Plans. If maintenance funds for CbT-RIF projects are not programmed and provided from the parent Service, CbT-RIF can be used to fund maintenance costs for those CbT-RIF-funded items during the year of purchase and the subsequent year as a temporary measure to permit the Service adequate time to program life-cycle costs. The fund is not intended to subsidize ongoing projects, supplement budget shortfalls, or support routine activities, which are a Service responsibility. Requests must be submitted through the responsible MAJCOM and GCC, per GCC policies, to the Joint Staff. Submission instructions are outlined in CJCSI 5261.01E, *Combating Terrorism Readiness Initiatives Fund.*

A4.4.1. **Emergency CbT-RIF Requirement.** An unanticipated requirement created by a combination of circumstances or the resulting state that requires immediate action to prevent, deter, or respond to a terrorist act.

A4.4.2. **Emergent CbT-RIF Requirement.** A newly formed, unexpected requirement resulting from a logical consequence of unforeseen circumstances calling for prompt action.

A4.4.3. GCCs must submit requests for CbT-RIF funds through CVAMP.

A4.4.4. Emergent requirements should be less than 2 years old. The requestor must have an approved, executable and exercised AT Plan.

A4.5. Effectively Managing the Resource Allocation Process.

A4.5.1. Ensure you plan for training and maintenance costs into the out years.

A4.5.2. The ATO needs to work closely with affected functional areas, installation financial advisors/comptroller and contracting from the beginning to address requirements. This will assist in identifying the appropriation sources and funding amounts.

A4.5.3. Adequately articulating and justifying requirements is crucial.

A4.5.4. Determine all appropriate potential funding sources and submit requests through the various channels. Once a requirement is funded by a source, cancel the other requests. **Note**: The Joint Staff does not allow the same request to be submitted through both the PPB&E and CbT-RIF process.

A4.5.5. There are organizations that can aid the commander in identifying technology to satisfy requirements: Physical Security Equipment Action Group (PSEAG), Technical Support Working Group (TSWG), AFSFC Concepts Division, Joint Requirement Office for Chemical, Biological, Radiological and Nuclear Defense (JRO-CBRND) and the Joint Non-Lethal Weapons Directorate (JNLWD). These organizations are separately funded to provide COTS information, rapid prototyping and research and development and/or evaluation of solutions for units in the field. They can provide information and research on technology and equipment evaluated and deemed suitable for your purpose. Additionally, they can provide field assessments to assist in identifying the optimal solutions to meet your requirements.

Attachment 5

AF APPROVED LEVEL II - ATO TRAINING SCHOOLS

A5.1. Attending any of the following schools may certify AF personnel for completion of Level II - ATO Training.

Table A5.1. Air Force Level II - ATO Training.

Air Combat Command 99th Security Forces Group Nellis AFB , NV Phone: DSN 682-1603
United States Air Force Expeditionary Center Ft Dix, NJ Phone: DSN 944-4101 (ext 185)
United States Air Force Special Operations School Hurlburt Field, FL Phone: DSN 579-6330
Air Force Reserve Command 610th Security Forces Squadron Conducts Mobile Training Team (MTT) courses Naval AS, Ft Worth TX Phone: DSN 739-5101 (ext 141, 134, 127)
US Air Forces in Europe Ramstein AB, GE Phone: DSN 314 480-6006
90th Ground Tactical Training Squadron F.E. Warren AFB, WY Phone: DSN 481-7629
96 Ground Combat Training Squadron (GCTS) Eglin AFB, FL Conducts MTT courses Phone: DSN 872-6172
PACAF Regional Training Center

736 SFS/Commando Warrior Andersen AB GU Phone: DSN 315 366-6087
PACAF ANSER MTT 25 E. Street Suite M-307 Hickam AFB, HI Phone: DSN 315 448-2481

Attachment 6 (Added-ACC)

ACC INSTALLATION ANTITERRORISM PLAN TEMPLATE

A6.1. (Added-ACC) AT Plan Template. This plan applies to all personnel assigned or attached to the installation. This plan is the overarching document that ensures tasks are aligned at all levels of command with emphasis on the individual member's understanding of their role in the base AT plan. Task all units for support, ensuring all organic, tenant, and supported units are considered.

ADD APPROPRIATE CLASSIFICATION MARKINGS/DeCLASS Instructions

NOTE: JCS-Approved AT Plan Template Format

Copy no. ____of_____ Copies

Base

Name/Location

Date/Time Group

(INSTALLATION NAME) ANTITERRORISM PLAN (AT 10-245)

Task Organization: [Include all agencies/personnel (base and civilian) responsible to implement the plan. Include as a separate Annex.] See Annex A (Task Organization).

Maps/Charts: (List all applicable maps or charts. Include enough data to insure personnel are using the right year/edition/version of the subject material.)

Time Zone: (Enter the time zone of the installation. Indicate the number of hours to calculate ZULU time.)

Ref: (Enter the compilation of pertinent publications, references, MOU/MOA/MAA. This list may be included in a separate Annex.) See Annex Q (References).

1. SITUATION:

a. **General.** (This plan applies to all personnel assigned or attached to the installation. Describe the political/military environment in sufficient detail for subordinate commanders, staffs, and units to understand their role in the installation AT operations.)

b. **Enemy.** (The enemy is any adversary capable of threatening the installation's personnel, facilities and equipment. Enter the general threat of terrorism, including transnational, to this installation including; the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces. Include the general threat of terrorist use of WMD against this installation. This information should remain unclassified when possible. See Paragraph 1f, Intelligence, on identifying specific threats. This information may be included as a separate Annex.) See Annex B (Intelligence).

c. **Friendly.** (Enter the forces available, both military and civilian, to respond to a terrorist attack. Include the next higher headquarters and adjacent installations, and any units/organizations that are not under installation command, but may be required to respond to such an incident. These units/organizations may include HN and US military police forces, fire and emergency services, medical, federal/state and local agencies, special operations forces, engineers, WMD detection, EOD, and decontamination. **Include MOAs/MOUs** and any other special arrangements that will improve forces available to support the plan.) (If CONUS, the Department of Justice, Federal Bureau of Investigations (FBI), is responsible for coordinating all federal agencies and DOD forces assisting in the resolution of a terrorist incident. If OCONUS, the Department of State is the lead agency.) This information can be included as a separate Annex(s). See Annex A (Task Organization) and Annex J (Command Relationships).

d. **Attachments/Detachments.** (Enter base/civilian agencies **not** normally assigned to the base that will be needed to support this plan. Explain interagency relationships and interoperability issues. List appropriate MOAs as necessary.) This can be listed in other Annex(s). See Annex A (Task Organization) and Annex J (Command Relationships).

e. **Assumptions.** (Enter all critical planning and execution assumptions used as a basis for this plan. Assumptions are those factors that are unlikely to change during the implementation of the AT installation plan. Put another way, those factors that you must address to allow you to continue to plan. They may range from troop strength on base, major political/social environment in the surrounding area, or terrorists acquiring shoulder fired antiaircraft missiles.) Examples follow:

(1) The installation is vulnerable to theft, pilferage, sabotage, and other threats.

(2) An act of terrorism involving WMD can produce major consequences that will overwhelm almost immediately the capabilities of the installation.

(3) Security personnel, both military and civilian, may be insufficient to provide total protection of all installation resources. Therefore, the principal owner or user of a facility, resource, or personnel must develop adequate unit awareness and safeguard measures.

(4) No single unit on the installation possesses the expertise to act unilaterally in response to WMD attacks.

(5) If protective equipment is not available, responders will not put their own lives at risk.

(6) Local, nonmilitary response forces will arrive within (time) of notification.

(7) Units specializing in WMD response will arrive on-site within (number of hours based on installation location) of notification.

f. **Intelligence.** (Enter the person, staff, or unit responsible for intelligence collection and dissemination. The installation commander must have a system in place to access current intelligence. The installation should have a process in place for developing the installation's tailored threat assessment or "local threat picture." The installation's tailored threat assessment should be continuously evaluated, updated, and disseminated as appropriate, and as directed by the installation commander. The commander should determine the frequency and the means of dissemination of the installation’s tailored AT product.) This can be included in Annex B (Intelligence).

2. MISSION. (Enter a clear, concise statement of the command's mission and the AT purpose or goal statement supporting the mission. The primary purpose of the AT installation plan is to safeguard personnel, property, and resources during normal operations. It is also designed to deter a terrorist threat; to enhance security and AT awareness; and to assign AT responsibilities for all installation personnel.)

3. EXECUTION:

a. **Commander's Intent**. (Commander's vision on how he/she sees the execution of the unit's AT program.)

b. **Concept of Operations.** (Enter how the overall AT operation should progress. This plan stresses deterrence of terrorist incidents through preventive and response measures common to all combatant commands and services. During day-to-day operations, the installation should stress continuous AT planning and passive, defensive operations. This paragraph should provide subordinates sufficient guidance to act upon if contact or communications with the installation chain of command is lost or disrupted.)

(1) The installation's AT concept of operations should be phased in relation to pre-incident actions and post-incident actions utilizing the FPCON levels as a means of ramping the installation up from FPCON NORMAL through consequence management actions. AT planning and execution requires that staff elements work with a much greater degree of cohesiveness and unity of mission than that required during the conduct of normal base sustainment operations. The AT mission, and the unpredictability of its execution, requires very specific "how to" implementation instructions of DOD FPCON measures and in what manner these actions must be coordinated. The implementation instructions are put into the form of action sets and can be displayed in the form of an execution matrix Pre-Incident Action Set Matrix).

(2) In Post-Incident planning, the installation should focus on its response and reconstitution responsibilities upon notification of a terrorist incident and the procedures for obtaining technical assistance/augmentation if the incident exceeds the installation's organic capabilities. National level responders (Federal Emergency Management Agency (FEMA), Red Cross, and FBI) may not be immediately accessible or available to respond to an installation's needs. Therefore, each installation must plan for the worst-case scenario by planning its response based on its organic resources and available local support through MOA/MOUs.

(3) The situation may dictate that the installation not only conduct the initial response, but also sustain response operations. This paragraph will include specific implementation instructions for all functional areas of responsibility and the manner in which these actions must be coordinated. The implementation instructions will be put in the form of action sets and displayed in the form of a synchronization matrix broken down by FPCONs. The synchronization matrix format must clearly describe relationships between activities, units, supporting functions, and key events which must be carefully synchronized to minimize loss of life and to contain the effects of a potential terrorist incident.

c. **Tasks.** (Enter the specific tasks for each subordinate unit or element listed in the Task Organization paragraph. Key members of the installation have responsibilities that are AT and/or WMD specific. The commander should ensure that a specific individual/unit/element within the installation is responsible for each action identified in this plan. Each individual/unit/element must know the tasks and responsibilities, what these responsibilities entail, and how these will be implemented. The AT Planning and Response Elements will be delineated in the Pre- and Post-incident Action Set Matrices. It is recommended that the installation commander identify/designate the primary lead for each element and enter that information in this paragraph.)

d. **Coordinating Instructions.** (This paragraph should include AT specific coordinating instructions and subparagraphs, as the commander deems appropriate. In addition, this section of the AT plan outlines aspects of the installation's AT posture that require particular attention to guarantee the most effective and efficient implementation of the AT plan. For the purposes of this plan, there are five basic coordinating instructions (1) AT Planning and Response Elements, (2) Procedural; (3) Security Posture; (4) Threat Specific Responsibilities and (5) Special Installation Areas. The sections listed below are representative, and may not be all-inclusive.)

(1) **AT Planning and Response**. For instructional purposes, this section provides an overview of AT Planning and Response Elements on the installation that is required to respond to a terrorist/WMD incident. Initial and sustained response to an attack must be a coordinated effort between the many AT Planning and Response Elements organic to the installation, based on the installation's organic capabilities. As the situation exceeds the installation's capabilities, it must activate MOAs/MOUs with the local/state/federal agencies. For the purposes of this plan, an installation's capability is divided into AT Planning and Response Elements. These tailored installation-level elements parallel the national-level FEMA elements and Defense Threat Reduction Agency's Joint Staff Integrated Vulnerability Assessment (JSIVA) response criteria. They may be used in conjunction with FPCON measures as appropriate. The AT Planning and Response Elements that need to be addressed are:

(a) Information and Planning * (POC: XP)

(b) Communications * + (POC: SC)

(c) HAZMAT * (POC: CE)

(d) Security * + (POC: SF)

(e) Fire Fighting * + (POC: CE)

(f) Health & Medical Services * + (POC: SG)

(g) Resource Support * (POC: LG)

(h) Mass Casualty Care * (POC: SG)

(i) Public Works Emergency Support * (POC: CE)

(j) Intelligence Process + (POC: IN)

(k) Installation AT Plans/Programs + (POC: XP)

(l) Installation Perimeter Access + (POC: SF)

(m) Security System Technology + (POC: SF)

(n) Executive Protection + (POC: SF)

(o) Response and Recovery + (POC: CE)

(p) Mail Handling + (POC: SC)

(*) Derived from FEMA Emergency Support Functions

(+) Derived from JSIVA assessment criteria

(2) **Procedural.** This area addresses alert notification of response forces and the base populace to defend against identified threats and activation of response forces.

(a) Alert Notification Procedures. See Appendix 14 to Annex C (POC: Command Post).

(b) Use of Force/Rules of Engagement. See Annex H (POC: Legal).

(c) Installation AT Training and Exercises. See Annex N (AT Training and Exercises). (POC: XP)

(d) Incident Response. See Appendix 1 to Annex C (POC: SF).

(e) Consequence Management. See Appendix 1 to Annex C (POC: CE).

(f) High Risk Personnel Protection Procedures. See Appendix 9 to Annex C (POC: SF).

(g) AT Program Review. (POC: XP)

(3) **Security Posture Responsibilities (POC: SF)**

(a) Law Enforcement. See Appendix 7 to Annex C.

(b) Perimeter Physical Security to include Lighting, Barriers, Access Control. See Appendix 6 to Annex C.

(c) Other On-site Security Elements. See Appendix 8 to Annex C.

(d) Operations Security. See Appendix 10 to Annex C.

(e) Technology. See Appendix 15 to Annex C.

(f) EOC Operations. See Appendix 12 to Annex C.

(4) **Threat Specific Responsibilities (POC: XP)**

(a) Installation Antiterrorism Program Structure. See Appendix 2 to Annex C.

(b) Weapons of Mass Destruction. See Appendix 5 to Annex C.

(c) Special Threat Situations. See Appendix 3 to Annex C.

(d) Information Security. See Appendix 11 to Annex C.

(5) **Special Security Areas (POC: SF)**

(a) Airfield/Flightline Security. See Appendix 4 to Annex C.

(b) Waterway/Port Security. See Appendix 4 to Annex C.

(c) Passenger Terminal Embarkation/Arrival Areas. See Appendix 4 to Annex C.

(d) Building Manager Responsibilities. See Appendix 4 to Annex C.

4. LOGISTICS AND ADMINISTRATION. (Enter the administrative and logistics requirements to support the AT plan, which should include enough information to make clear the basic concept for planned logistics support. Ensure the staff conducts logistical planning for both pre- and post-incident addressing; as an example, the following considerations: vehicle support to security forces, locations of consolidated WMD defense equipment, expedient decontamination supplies, Individual Protective Equipment exchange points, special contamination control requirements, retrograde contamination monitoring sites, WMD equipment/supply controlled supply rates and pre-stockage points, and procedures for chemical defense equipment "push" packages. Specific logistics and administrative requirements will emerge throughout the planning process outlined in the concept of operations, specifically when developing the action sets. In summary, any logistical action to support the AT/FP plan from pre-incident through incident recovery should be addressed.)

a. **Administration.** See Annex (Personnel).

b. **Logistics.** See Annexes D (Logistics) and E (Fiscal).

5. COMMAND AND SIGNAL. (Enter instructions for command and operation of communications-electronics equipment. Identify the primary and alternate locations of the command post, battlestaff and DCG. Record the installation's chain of command. Highlight decision-making processes for FPCON changes and alert notifications. The chain of command may change based on the deployment of a Joint Task Force or a National Command Authority-directed mission. Identify the location of chemical staffs or any technical support elements that could be called upon in the event of a terrorist WMD incident and the means to contact each. The installation must provide for prompt dissemination of notifications and alarm signals, and the timely/orderly transmission and receipt of messages between elements involved in and responding to an incident and/or FPCON change.)

a. **Command.** See Annex A (Task Organization) and Annex J (Command Relationships).

b. **Signal.** See Annex K (Communications).

c. **Command Centers:**

(1) **Command Post:** (Enter primary and alternate locations, phone numbers, email addresses, and additional contact information)

(2) **BattleStaff:** (Enter primary and alternate locations, phone numbers, email addresses, and additional contact information)

(3) **Disaster Control Group:** (Enter primary and alternate locations, phone numbers, email addresses, and additional contact information)

d. **Succession of Command:** (Describe the succession of command.)

//SIGNATURE//

Wing Commander

Signature Block

ANNEXES: (Should provide amplifying instructions on specific aspects of the plan. Each ANNEX can be subdivided into APPENDICES, TABS, and ENCLOSURES as required to provide amplifying instructions. Further, some of these supporting documents may be established in other unit operating orders/procedures and referenced as required.)

ANNEX A - Task Organization (Enter key AT organization composition: TWG, FPWG, FPEC, Crisis Management Team, Emergency Operations Center, First Response Elements, etc.)

Appendix 1 - **Table of Organization**

Appendix 2 - **Post Prioritization Chart**

ANNEX B - Intelligence (Enter the agency(s) responsible for intelligence and specific instructions.)

Appendix 1 - **Local Threat Assessment (include national threat assessment)**

Appendix 2 - **Local WMD Assessment**

Appendix 3 - **Local Criticality/Vulnerability Assessment**

Appendix 4 - **Risk Assessment**

Appendix 5 - **Predeployment AT Vulnerability Assessments** (Process for ensuring deploying personnel receive Area of Responsibility specific briefing on destination location.)

ANNEX C - Operations (Annex C and supporting Appendices will provide specific instructions for all the various AT operations. All other Annexes/Appendices support the implementation of Annex C.)

Appendix 1 - **Incident Planning and Response** (Enter how the various agencies, military and civilian, and resources will be integrated to respond to the operations outlined below. These instructions should be generic enough to apply across the operational spectrum. Specific instructions for each operation will be detailed in the appropriate Annex/Appendix/Enclosure.)

Tab A - Incident Command and Control Procedures (POC: XP)

Tab B - Incident Response Procedures (POC: SF)

Tab C - Consequence Management Procedures (POC: CE)

Appendix 2 - **Antiterrorism**

Tab A - Protection Level Assets and Critical Facilities (Mission Essential Vulnerable Assets)

(POC: SF)

Tab B - Potential Terrorist Targets (POC: AFOSI Det)

Tab C - FORCE PROTECTION CONDITIONS

Enclosure 1 - FORCE PROTECTION CONDITION Action Sets (POC: XP) (Provides a consolidated listing of all unit specific FPCON actions by FPCON. When attached to AT plan, the overall plan becomes “CONFIDENTIAL.” Limit dissemination of this enclosure to decision making bodies.)

Tab D - Random Antiterrorism Measures (RAM) Procedures (POC: XP)

Tab E - Unit Specific FPCON checklists (POC: Units) (Units will only have their checklist in their copy of the plan. Key leadership and decision making bodies will maintain a copy of all unit checklists. When all checklists are attached to the AT plan, the overall plan becomes “CONFIDENTIAL.” Limit dissemination of this enclosure to decision making bodies.)

Tab F - Areas of Responsibility (Pictorial map showing areas of base units provide AT surveillance coverage.) (POC: XP)

Appendix 3 - **Special Threat Situations** (POC: SF)

Tab A - Bomb Threats

Enclosure 1 - Bomb Threat Mitigation

Enclosure 2 - Evacuation Procedures

Enclosure 3 - Search Procedures

Tab B - Hostage Barricaded Suspect

Appendix 4 - **Special Security Areas** (POC: SF)

Tab A - Flightline/Airfield Security (to include MANPAD threat/mitigation to arrival and departure corridors) Note: modeling simulation software can be downloaded at http://msic.dia.smil.mil/mshome pages/fptas/

Tab B - Waterway/Port Security

Tab C - Passenger Terminal Embarkation/Arrival Areas

Tab D - Building Manager Responsibilities.

Tab E - On-base school FPCON Support

Appendix 5 - **Weapons of Mass Destruction and HAZMAT** (Enter the specific procedures, planning, training, and response to WMD incidents. Care should be taken to integrate existing plans for response to HAZMAT incidents to avoid duplication. Include "baseline" preparedness.)

Tab A - WMD Action Set Synchronization Matrix

Tab B - WMD Detection Equipment Availability, Maintenance and Calibration

Tab C - WMD Protection and Response Equipment Availability

Appendix 6 **- Food and Water Security Procedures** (Action sets to ensure food and water sampling to meet increased threat.) Ensure all affected agencies (CE, FSS, SF, and SG) are involved in this annex.

Appendix 7 - **Installation Security Plan (Physical Security)**

Tab A - Installation Barrier Plan (Enter procedures and pictorial representation of barrier plan.)

Tab B - Construction Considerations

Tab C - Facility and Site Evaluation and/or Selection

Tab D - AT Guidance for Off-Installation Housing

Appendix 8 - **Law Enforcement**

Tab A - Organization, training, equipping of augmentation security forces

Tab B - Alternate Dispatch Location

Tab C - Alternate Arming Point (Armory) Procedures

Tab D - Liaison with local, state, federal law enforcement agencies (List contact information)

Tab E - Dissemination procedures for Law Enforcement Sensitive information

Appendix 9 - **Other On-Site SF**

Appendix 10 - **High Risk Personnel**

Tab A - List of High Risk Billets

Appendix 11 - **AT Operations Security**

Appendix 12 - **AT Information Security**

Appendix 13 - **Battlestaff and DCG Operations** (Procedure for the activation and operation of the Battlestaff and DCG.)

Tab A - Battlestaff/DCG Staffing (Partial/Full)

Tab B - Battlestaff/DCG Facility Layout

Tab C - Battlestaff/DCG Communications Procedures (Outline command and control, battlestaff directive release, FPCON change process, address alternate plans and backup procedures, etc.)

Tab D - Battlestaff/DCG Briefing Procedures

Tab E - Battlestaff/DCG Situation Boards

Tab F - Battlestaff/DCG Security and Access Procedures Tab G - Battlestaff/DCG Transportation

Appendix 14 - **Critical Systems Continuity of Operations Plans** (Enter those systems that are essential to mission execution and infrastructure support of the installation.)

Tab A - List of installation critical systems. Ensure the plan identifies critical infrastructure and supports the Critical Infrastructure Program (CIP) as outlined in AFPD 10-24 (1 Dec 1999). Examples include power, water, computer networks, communications, etc.

Tab B - Execution checklist for each critical system. (Address alternate plans and back-up procedures)

Tab C - Civilian Terrorist Targets. (Identify off-base facilities, that if attacked, could cause collateral damage to the installation populace. This tab should include a map with distances from the installation and specifics on the possible threat of contamination and collateral damage. Examples include: nuclear power plants, chemical refineries, hazardous materials storage areas, research and development facilities, dams, explosives storage or manufacturing facilities, etc. Utilize mapping technology like satellite imagery, GEO Base/Reach, Federal Mapping Agency, etc.)

Appendix 15 - **Emergency Mass Notification Procedures.** Enter the specific means and procedures for conducting a mass notification. Also covered should be the procedures/means for contacting key personnel and agencies.

Tab A - Situation Based Notification

Tab B - Matrix List of Phone Numbers/Email Accounts

Appendix 16 - **Exploit Technology Advances** (Enter the process and procedures for developing and employing new AT and FP technology.)

ANNEX D - Logistics (Specific logistics instructions on how to support AT operations)

Appendix 1 - **Priority of Work** (Enter the priority of employing scarce logistical resources.)

Appendix 2 - **Emergency Supply Services**

Appendix 3 - **Weapons and Ammunition Supply Services**

Appendix 4 - **Emergency Equipment Services**

Appendix 5 - **Evacuation Shelters**

Appendix 6 - **Generator Refueling Matrix**

ANNEX E - Fiscal (Specific fiscal instructions on how to support AT operations from pre-incident through post-incident. Include AT unfunded process and CbT RIF submission staffing process.)

ANNEX F - TENANT Commanders (Specific instructions on how tenant commands/agencies support AT operations and participate in base AT organizational structure.)

ANNEX G - Air Operations (Specific air instructions on how to support AT operations)

Appendix 1 - **List of Landing Zones** (Used for emergency medical evacuations or equipment/ personnel staging areas.)

Appendix 2 - **Landing Zone Preparation Procedures** (Marking, communications, signals, etc)

Appendix 3 **- Antihijacking Procedures**

ANNEX H - Legal (Enter the jurisdictional limits of the installation's commander and key staff. Although the Department of Justice, FBI, has primary law enforcement responsibility for terrorist incidents in the United States, the installation commander is responsible for maintaining law and order on the installation. Once a task force or other than installation support arrives on the installation, these agencies should maintain close coordination with the local incident commander. In all cases, command of military elements remains within military channels. Include established Rules for Use of Force and Rules of Engagement and legal reviews of overwatch positions.)

Appendix 1 - **Jurisdictional Issues**

Appendix 2 - Rules for **Use of Force (CONUS) and/or Rules of Engagement (OCONUS) Instructions**

Appendix 3 - **Pictorial Representation of Installation Jurisdiction**

ANNEX I - Public Affairs (Specific Public Affairs Officer instructions on how to support AT operations)

Appendix 1 - **Public Affairs Organization and Operation**

Appendix 2 - **Local/Regional Media Contact Information**

Appendix 3 **- Information Warfare** (AT Deterrence Activities and Information Release)

ANNEX J - Command Relationships (Provides specific guidance on command relationships and interoperability issues, incident command and control, military/civilian interoperability)

Appendix 1 - **AT Organizational Charts** (Examples: Crisis Management Team, FPWG, TWG, First Response Element, Incident Command Organization, civilian and other external agencies critical to AT plans.)

ANNEX K - Communications (Specific communications instructions on how to support AT operations. Include systems/procedures for SECURE and NON-SECURE communications means.)

Appendix 1 - **Installation AT Communications Architecture**

Appendix 2 - **Incident Command Communications Architecture**

Appendix 3 - **Battlestaff/DCG Communications Architecture**

Appendix 4 - **SF Communications Architecture**

Appendix 5 - **Fire Department Communications Architecture**

Appendix 6 - **Medical Communications Architecture**

Appendix 7 - **Other AT Agencies**

ANNEX L - Health Services (Specific medical instructions on how to support AT operations) (Note: may be sufficient to refer to medical treatment facility's Medical Contingency Response Plan rather than stand alone annex)

Appendix 1 - **Mass Casualty Plan**

Appendix 2 - **Procedures for Operating with Civilian Emergency Medical Service and Hospitals**

ANNEX M - Safety (Specific safety instructions on how to support AT operations and exercises)

ANNEX N - Training and Exercises

Appendix 1 - **AT Required Training**

Appendix 2 - **Exercises**

ANNEX O - Personnel Services (Enter administrative and personnel procedures required to support the plan e.g., civilian overtime, post-event counseling, post-traumatic stress syndrome counseling, etc.)

Appendix 1 - **Operating Emergency Evacuation Shelters**

ANNEX P - Reports (Enter all the procedures for report submissions and report format.)

Appendix 1 - **Reporting Matrix**

ANNEX Q - Weather (Required actions by the weather flight and/or NAF Operational Weather Squadron to provide weather support products to support AT operations)

ANNEX R - References (Enter all supporting reference materials, publications, regulations etc.)

ANNEX U - Distribution (Enter the list of agencies to receive this plan. Annotate plan classification, handling and declassification procedures.)

ADD APPROPRIATE CLASSIFICATION MARKINGS/DeCLASS Instructions

ATTACHMENT 7 (Added-SHAWAFB)

UNIT ANTITERRORISM OFFICER APPOINTMENT MEMORANDUM

MEMORANDUM FOR 20 FW/CCFP

FROM:

SUBJECT: Letter of Appointment for Unit Antiterrorism Officers

1. In accordance with AFI 10-245, para 1.2.18 and 2.9 as supplemented, the following individuals are appointed as Unit Antiterrorism Officers (UATOs) for (Unit). Direct questions or comments concerning the wing's Antiterrorism Program to them.

<u>PRIMARY</u> <u>ALTERNATE</u>

Rank/Name:
Office Symbol:
NIPRNET Address:
SIPRNET Address:
Duty Phone:
Antiterrorism
Training date:

2. This letter supersedes all previous letters referencing this subject.

Commander

ATTACHMENT 8 (Added-SHAWAFB)

UNIT ANTITERRORISM OPERATING INSTRUCTION

OPR: 88 XXX/Office Symbol (Rank Name) **Certified by: (Your Sq)/CC**
This is an initial publication **Pages: X**

OR
Supersedes: OI 31-210, XX Month XXXX

This instruction establishes procedures regarding **(Your Sq)** implementation of the XX FW Antiterrorism Plan. This operating instruction (OI) implements unit level procedures IAW the XXXXXXX Air Force Base Supplement to AFI 10-245_ACCSUP1 and The XX FW Antiterrorism/Force Protection Program. **(If initial publication)**

SUMMARY OF REVISIONS:

Here's where you say what's been revised. **(If revising an existing publication) Or: this is an initial publication and must be read in its entirety.**

1. Wing RAM implementation.

1.1. Wing Random Antiterrorism Measures (RAM) implementation.

1.1. Wing level RAMs will be implemented IAW the XX FW Antiterrorism Plan. The unit commander will implement actions based on the Wing RAMs but may add additional items or procedures under the applicable measures.

1.1.2. State how your squadron personnel are notified when there is a RAM implemented. (i.e. who is notified and who is responsible for accomplishing the RAM, Facility Manager, Unit Security Monitor, or Unit ATO).(Note: If your unit has more than one facility, all facilities within your unit must accomplish the RAM)

1.1.3. After a RAM has been completed, it must be annotated in a log maintained by the Facility Manager/Unit Security Monitor/Unit ATO, whichever is applicable. The RAM log will be maintained for one year and a copy sent monthly to the XX FW/ATO.

1.1.4. The Unit ATO will also inform their Unit Control Center (UCC) when all RAM actions are completed. The UCC will also maintain a log of completed RAMs.

1.2. **Dissemination of FPCON changes.** Dissemination of FPCONs must be a quick and flawless system. To facilitate this, the UCC will be responsible to notify the whole squadron. Upon notification of a FPCON change, the UCC will implement pyramid recall procedures. If telephonic contact is not possible, runners will be used. The UCC will notify the outlying sections/facilities within the unit. (List facilities and phone numbers to contact)

2. Unit Antiterrorism Officer (UATO) duties and responsibilities.

2.1. A primary and alternate unit antiterrorism officer will be appointed in writing and a copy of the letter forwarded to XX FW/ATO.

2.2. The Antiterrorism monitor will be responsible for managing all unit antiterrorism actions and administration to include implementation of RAMs, increased FPCONs, and training.

2.3. The Unit antiterrorism monitor will maintain:

2.3.1. Appointment letters.

2.3.2. AFI 10-245, Air Force Antiterrorism Standards, as supplemented.

2.3.3. Wing Antiterrorism Plan (Basic Plan)

2.3.4. This operating instruction.

2.3.5. FPCON visual aids (XAFBVA 10-2, XAFBVA 10-3, and XAFBVA 10-4).
These aides are available from XX FW/ATO

2.3.6. Unit/Building specific checklists for implementation for each FPCON.

2.3.7 Detailed checklists for any tasking the unit is responsible for carrying out in support of the Installation Antiterrorism Plan. (ie Augmentee program, manning or equipment support)

3. Antiterrorism/Force Protection Level 1 Training Tracking Plan. The following guidance will be used to ensure XX SVS personnel receive the proper training for AT Level 1.

3.1. All unit members must receive AT Level 1 training annually.

3.2. The (**appointed person/section**) will ensure that unit members departing overseas for temporary duty (TDY), overseas leave, or permanent change of station (PCS) have completed Level I training within 3 months of departure. Additionally, members must receive a threat briefing for the deployed location from AFOSI Detachment XXX within three months of departure.

3.3. To meet the current training requirement, PCS, TDY, overseas leaves, and deployment out-processing checklists will include annotation of AT Level I training.

3.4. The (**appointed person/section**) will be responsible to schedule and track all Level I AT/FP training.

3.5. The **(appointed person/section)** will forward a report quarterly listing all AT Level I training to XX FW/ATO.

3.6. For squadrons who deploy as a unit, your will be responsible to ensure your unit has enough Level II certified individuals to be assigned as the deployed ATO.

3.6.1. Ensure your deployed ATO is briefed on their responsibilities. The Deployment ATO must ensure their personnel have had their Level I training documented. Ensure all personnel deploying have received their AOR Specific information. Obtain the itinerary of the route taken to the AOR. The Deployed ATO should research all areas being traversed so the team will be prepared in case of a layover. Research should include information on the terrorist environment of the country, specifically what groups are present and how active they are. Cultural idiosyncrasies of that country, and places available to seek assistance (ie..Military installations, Embassies and Consulates). Obtain a Vulnerability Assessment of the deployed site and plan accordingly. This information is available at the Theater websites on the NIPRNet and SIPRNet. Deployed ATOs should also look up the DoD Foreign Clearance Guide for information on possible additional paperwork which may be required for entry into the country.

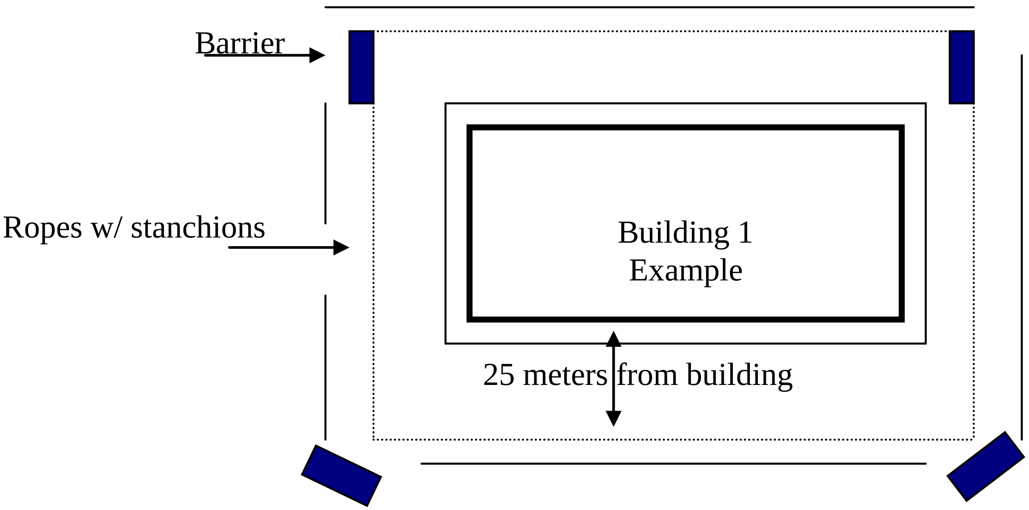
4. Unit Facility Barrier Plans.

4.1 List of equipment (i.e. barriers, stanchions, rope, signs, etc.) for blocking off parking lots and state where the equipment is located.

4.2. State who is responsible for placing the barriers, stanchions, etc. in place

4.3. Provide drawings for each facility within the unit and how the barriers will be placed.

4.3.1. Building 1:



4.4. Those tasked with implementing the unit barrier plan will have to ensure all personnel parked within the 25 meter standoff area is notified to move them. The unit should also have a plan in place for vehicles within the 25 meters without an identified owner (ie.. contacting a tow truck to have it removed).

4.5 For facilities on the Installation Barrier Plan, the unit will be responsible for accomplishing the above items with temporary materials until the permanent barriers arrive.

5. Building Evacuation Procedures. Unit ATOs are responsible to ensure all facilities in their unit have an appointed person/section as a Point of Contact (POC) for all evacuation procedures.

5.1. Bomb Threat Procedures.

5.1.1. The **(appointed person/section)** is responsible for ensuring all facilities in the unit have a bomb threat evacuation plan. The plan should identify a primary and alternate rally point. Rally points should not be located in parking lots full of vehicles, an open area or adjacent building is preferable. This makes it harder for someone to preposition an explosive device. All facility managers must ensure the evacuation routes are clear of obstructions to facilitate the evacuation. Identify personnel responsible for ensuring all occupants have evacuated the building, and appoint someone to search and clear the rally point prior to use. The plan should also have provisions to ensure all occupants are accounted for. The primary and alternate rally points have been identified for each building as an attachment to this plan keeping them at least 500feet from the building (remember to change area after each exercise or alarm.)

5.1.2. For facilities with multiple organizations residing in one building, evacuations must be coordinated to ensure all occupants are accounted for. State **(what section or who)** will alert all personnel inside the building of a bomb threat to your building or area.

5.2. Suspicious Package Procedures

5.2.1. The **(appointed person/section)** is responsible for ensuring all personnel have evacuated the building and who will search and clear the rally point prior to use.

5.2.1.2. State **(what and who)** will alert all personnel inside the building of a suspicious package.

5.2.1.3. Inform evacuees where the suspicious package is located and ensure personnel do not evacuate through a potential danger/contaminated area.

5.2.2. State where the rally point will be, keeping them at least 500 feet from the building (remember to have several areas and to change area after each exercise or alarm.)

5.2.3. Identify all personnel who may have come in contact with the suspicious package and keep them isolated from other evacuees to avoid cross-contamination.
5.2.4. State how notification will be made of a suspicious package to your building or area.

5.3. Fire Procedures.

5.3.1. The **(appointed person/section)** is responsible for ensuring all personnel have evacuated the building, i.e. conducted a head count at the rally point.

5.3.2. State **(what and who)** will alert all personnel inside the building of a fire.

5.3.3. State where the rally point will be, ensure to maintain a clear avenue of approach for the first responders.

5.3.4. State how notification to all appropriate agencies will be made of a fire alarm at your building or area.

6. **Augmentee Program**.

6.1. State how you are going to ensure enough personnel are trained and available for the Installation Augmentee program. Unit monitors must maintain an up to date list of personnel who have been through the training. If the numbers of personnel drops below the level of the requirement due to PCS/Separations or deployments, the Unit ATO is responsible for contacting Security Forces for the next available class.

7. Unit AT Funding:

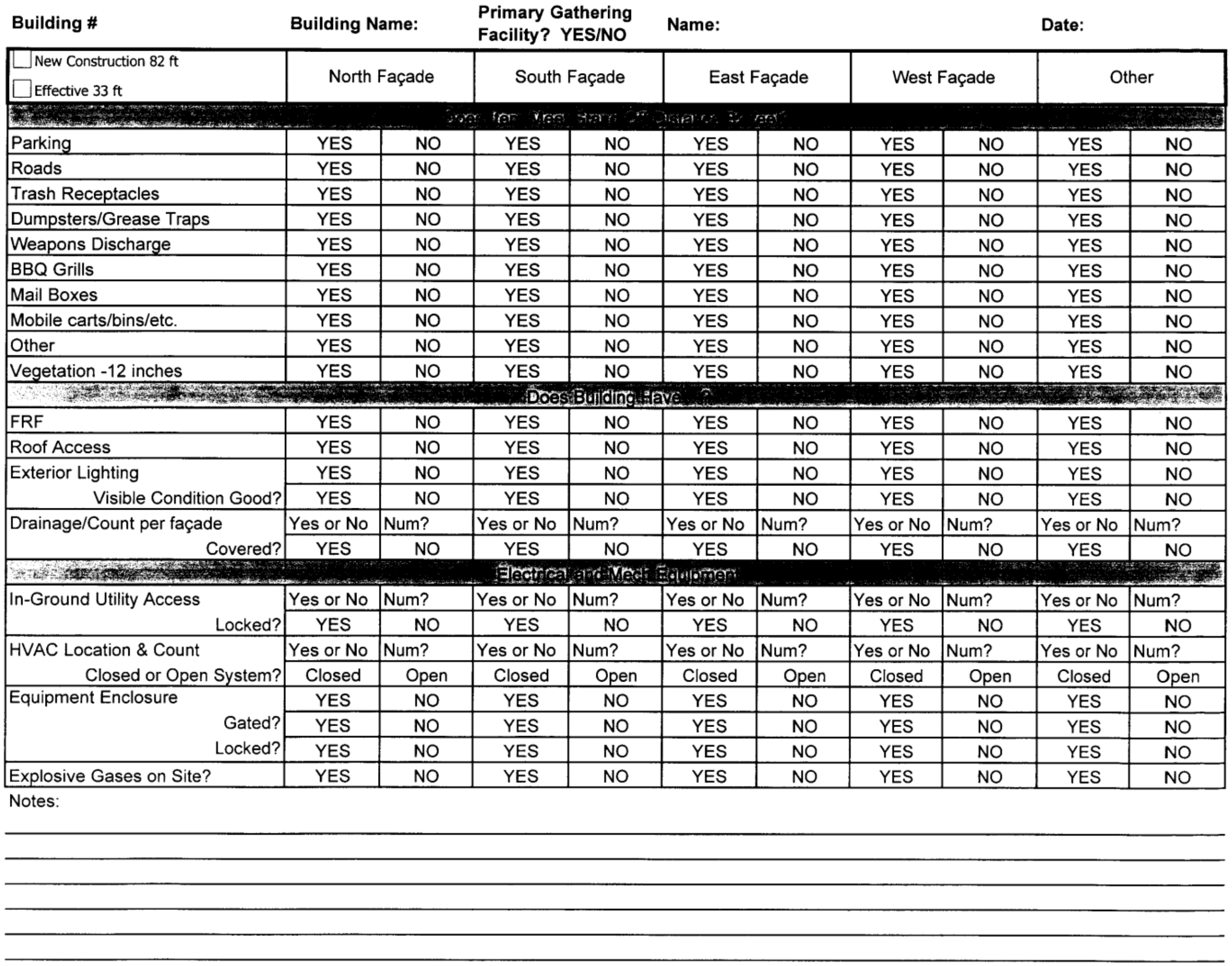
7.1. Unit Antiterrorism improvements will be funded at the lowest possible level. If the squadron can fund small projects, (ie locks, alarms etc.) it will be the first option. Any project which cannot be funded through the squadron will be submitted through the Installation ATO.

7.2. Any equipment or project that is funded through Installation Antiterrorism funds must be submitted to the Unit ATO for submission to the XX FW/ATO to be presented during a force Protection Working Group meeting.

JOE DOE, Major, USAF
Commander

ATTACHMENT 9 (Added-SHAWAFB)

FACILITY SECURITY CHECKLIST



Building # Building Name: Primary Gathering Facility? YES/NO Name: Date:

□ New Construction 82 ft □ Effective 33 ft	North Façade		South Façade		East Façade		West Façade		Other	
Does Item Meet Stand Off Distance to Asset?										
Parking	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Roads	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Trash Receptacles	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Dumpsters/Grease Traps	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Weapons Discharge	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
BBQ Grills	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Mail Boxes	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Mobile carts/bins/etc.	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Other	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Vegetation -12 inches	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Does Building Have ?										
FRF	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Roof Access	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Exterior Lighting	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Visible Condition Good?	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Drainage/Count per façade	Yes or No	Num?	Yes or No	Num?	Yes or No	Num?	Yes or No	Num?	Yes or No	Num?
Covered?	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Electrical and Mech Equipment										
In-Ground Utility Access	Yes or No	Num?	Yes or No	Num?	Yes or No	Num?	Yes or No	Num?	Yes or No	Num?
Locked?	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
HVAC Location & Count	Yes or No	Num?	Yes or No	Num?	Yes or No	Num?	Yes or No	Num?	Yes or No	Num?
Closed or Open System?	Closed	Open	Closed	Open	Closed	Open	Closed	Open	Closed	Open
Equipment Enclosure	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Gated?	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Locked?	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Explosive Gases on Site?	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO

Notes:

ATTACHMENT 10 (Added-SHAWAFB)

PROGRAM ASSISTANCE CHECKLIST

ANTITERRORISM (AT)

PROGRAM ASSISTANCE VISIT (PAV)

UNIT: ____________________

NAME:_________________ DUTY TITLE:________________ DATE:____________

UNIT AT REPRESENTATIVE:_______________________________________

1.	**AT PROGRAM:**	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
1.1	Does the unit have a letter identifying a Primary & Alternate AT representative signed by the commander? (AFI 10-245_SHAWAFBSUP1, paragraph 1.2.20.4)			
1.2	Are the personnel assigned as UATOs in the grade of E-5 or above? (AFI 10-245_SHAWAFBSUP1, paragraph 1.2.20.4)			
1.3	Has a copy of the AT/FP representative letter been forwarded to 20 FW/ATO? (AFI 10-245_SHAWAFBSUP1, paragraph 1.2.20.4)			
1.4.	Has the commander ensured Physical Security Evaluations on unit facilities have been conducted/reviewed annually and filed using DD Form 2367? (AFI 10-245_SHAWAFBSUP1, paragraph 1.2.20.7)			
1.5.	Does the unit ATO maintain a Unit AT Program book? (AFI 10-245_SHAWAFBSUP1, paragraph 1.2.20.6)			
1.5.1.	Does the unit AT Program Book contain A current unit AT/FP Monitor letter signed by the unit commander? (AFI 10-245_SHAWAFBSUP1, Attachment 11)			

1.5.2.	Does the Unit AT Program Book maintain a reference library containing the current AFI 10-245, *The Air Force Antiterrorism/Force Protection (AT/FP) Program Standards*, AFI 10-245_SHAWAFBSUP1, and 20 FW OPLAN 10-245, *Installation Antiterrorism Plan*? (AFI 10-245_SHAWAFBSUP1, Attachment 11) (This can be either by electronic or paper media.)			
1.5.3.	Does the AT Program Book contain facility maps identifying rooms and exterior storage rooms/facilities containing hazardous materials (ammunition, paints, gasoline, oils, or flammable solids) or explosive type materials under the unit's control? (AFI 10-245_SHAWAFBSUP1, Attachment 11)			
	AT PROGRAM (Cont.):	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
1.5.4.	Does the AT Program Book contain a list of unit-specific FPCON Measures, located in 20 FW OPLAN 10-245? (AFI 10-245_SHAWAFBSUP1, Attachment 11).			
1.5.5.	Does the AT Program Book contain written designation of storage location for FPCON signs? (AFI 10-245_SHAWAFBSUP1, Attachment 11)			
1.5.6.	Does the AT Program book contain a list of entrances/exits identified for posting or non-posting of FPCON signs? (AFI 10-245_SHAWAFBSUP1, Attachment 11, paragraph 13.1.7.)			
1.5.7.	Does the AT Program book contain Written directions of where the unit stores ropes, stanchions, traffic cones, and any other materials used in the event of initiating unit's parking plan during increased FPCONs? (AFI 10-245_SHAWAFBSUP1, Attachment 11)			
1.5.8.	Does the AT Program book contain Record of Facility Physical Security Assessments conducted on unit facilities? (AFI 10-245_SHAWAFBSUP1, Attachment 11)			
1.5.9.	Does the AT Program book contain monthly AT/FP Level I and II training statistics? (AFI 10-245_SHAWAFBSUP1, Attachment 11)			
1.5.10	Does the UATOs maintain an adequate supply of standardized FPCON signs? (AFI 10-245_SHAWAFBSUP1, paragraph 2.9.5.11)			

2.	**UNIT AT OPERATING INSTRUCTION (OI)**	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
2.1	Has the unit commander established a unit AT Operating Instruction? (AFI 10-245_SHAWAFBSUP1, paragraph 1.2.20.6)			
2.2	Does the unit AT OI contain the following:			
2.2.1	Bomb Threat/Evacuation procedures to include a Primary & Alternate rally point? (AFI 10-245_SHAWAFBSUP1, Attachment 8)			
2.2.2	Fire Evacuation procedures to include a Primary & Alternate rally point? (AFI 10-245_SHAWAFBSUP1, Attachment 8)			
	UNIT AT OPERATING INSTRUCTION (OI) (Cont.)	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
2.2.3	Accountability procedures for all types of evacuations, e.g., Bomb, Fire, Natural Disaster, etc.? (AFI 10-245_SHAWAFBSUP1, Attachment 8)			
2.2.4	Threat information dissemination procedures? (AFI 10-245_SHAWAFBSUP1, Attachment 8)			
2.2.5.	Does the OI address procedures for Facility Security Evaluations and Risk Assessment? (AFI 10-245_SHAWAFBSUP1, Attachment 8)			
2.2.6.	Does the OI address procedures for conducting and tracking ancillary training requirements for AT Level I and II training? (AFI 10-245_SHAWAFBSUP1, Attachment 8)			
2.2.7	Random Antiterrorism Measure (RAM) procedures? (AFI 10-245_SHAWAFBSUP1, Attachment 8)			
2.2.8.	Does the OI address a Parking Plan for use during increased Force Protection Conditions (FPCONSs)? (AFI 10-245_SHAWAFBSUP1, Attachment 8)			
2.2.9	Procedures to ensure the entire unit receive annual AT/FP Level I Awareness Training? (AFI 10-245_SHAWAFBSUP1, Attachment 8)			

3.	**UNIT RANDOM ANTITERRORISM MEASURE (RAM) PROGRAM**	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
3.1.	Does the unit AT/FP representative forward copies of RAMs conducted to group and wing ATOs? (AFI 10- 245_SHAWAFBSUP1, paragraph 2.9.5.13)			
4.	**BASE FORCE PROTECTION CONDITION (FPCON) CHECKLISTS**	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
4.1.	Does the unit have the current Base FPCON Checklists? (AFI 10-245_SHAWAFBSUP1, paragraph 2.22.4.1)			
4.2.	Does the unit have FPCON notification procedures established? (AFI 10-245_SHAWAFBSUP1, paragraph 2.22.4.1)			
5.	**UNIT AT TRAINING**	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
5.1.	Has the unit commander included Level I AT Awareness training in their Unit Master Training Plan? (AFI 10-245_SHAWAFBSUP1, paragraph 1.2.20.9)			
5.3	Is AT Level I Awareness Training tracked/documented the same as other ancillary training requirements? (AFI 10-245_SHAWAFBSUP1, paragraph 2.25.10.3)			
5.4.	Does the UATO provide annual AT training to unit personnel IAW AFI 10-245, paragraph 2.22? (AFI 10-245_SHAWAFBSUP1, par 2.9.5.9)			
5.5.	Does the unit ATO Maintain a stockpile of JS Guide 5260, *Service Member's Personal Protection Guide: A Self-help Handbook to Combating Terrorism*, and the *Antiterrorism Individual Protective Measures* folding card to issue one to each member of the unit? (AFI 10-245_SHAWAFBSUP1, paragraph 2.9.5.8)			
COMMENTS				

Attachment 11 (Added-SHAWAFB)

AT/FP PROGRAM BOOK CONTENTS

1. Unit-Level AT Representative's Program Continuity Book. Each unit AT monitor will maintain a program continuity book. As a minimum, the book will contain the following items:

1.1. A current unit AT monitor letter signed by the unit commander. This letter will include the facilities (by building number and if needed location) under the responsibility of the appointed individuals.

1.2. Maintain a reference library containing the current AFI 10-245_ACCSUP1_SHAWSUP1, *Antiterrorism*, and 20 FW OPLAN 10-245, *Installation Antiterrorism Plan*.

1.3. Facility maps identifying rooms and exterior storage rooms/facilities containing hazardous materials (ammunition, paints, gasoline, oils, or flammable solids) or explosive type materials under the unit's control.

1.4. Maintain a list of unit-specific FPCON Measures, located in 20 FW OPLAN 10-245, *Installation Antiterrorism Plan*

1.5. Maintain a list of Random Antiterrorism Measures (RAMs) for your unit's facilities. RAMs are explained in 20 FW OPLAN 10-245, *Installation Antiterrorism Plan*. DoD and Shaw Air Force Base FPCON measures are also listed in the 20 FW OPLAN 10-245, *Installation Antiterrorism Plan.*

1.6. Written designation of storage location for FPCON signs.

1.7. List of entrances/exits identified for posting of FPCON signs. Entrances/exits not normally used for day-to-day operations may be exempted from posting signs.

1.8. Approved Unit Parking Plan.

1.9. Written directions as to where the unit stores ropes, stanchions, traffic cones, and any other materials used in the event of initiating unit's parking plan during increased FPCONs.

1.10. Record of Facility Physical Security Assessments conducted on unit facilities.

Attachment 12 (Added-SHAWAFB)

RANDOM ANTITERRORISM MEASURE REPORT

MEMORANDUM FOR 20 FW/CCFP

FROM: (Unit)

SUBJECT: Monthly Random Antiterrorism Measures (RAMs) – (Month/year)

1. **REFERENCES:**

a. 20 FW/CC Ltr, Monthly Random Antiterrorism Measures (RAMs)

b. Unit FPCON Procedures and Checklists

2. Monthly Random Antiterrorism Measures (RAMs) tasked to (Unit) for (Month/year) were conducted as shown below:

Measure	Group	Unit/Facility	Time	Date
Control access to all facilities and implement 100% ID checks of personnel/conduct inspection of all hand-carried items—no exceptions (personal recognition is authorized for personnel entering their own unit work centers)	9 AF	ALL	0930-1330	8-Sep-09

OUTCOME:
SATISFACTORY. RAM was conducted without incident.
EVALUATOR: TSgt Steinert

Measure	Group	Unit/Facility	Time	Date
As a minimum, not to exceed two hours, inspect the interior and exterior of buildings (to include parking lots) in regular use for suspicious packages/activity	MXG	20 AMXS/ALL	1350-1550	11-Sep-09

OUTCOME:
SATISFACTORY. RAM was conducted without incident.
EVALUATOR: TSgt Derk

3. POC:

Commander,

Attachment 13 (Added-SHAWAFB)

CIVIL ENGINEER UFC 4-010-01 REQUIREMENT CERTIFICATION MEMORANDUM

MEMORANDUM FOR 20 FW/CC

FROM: 20 CES

SUBJECT: Certification of project _______________ to meet DoD Standards

1. The 20th Civil Engineering Squadron certifies project number ________ meets all DoD minimum Antiterrorism standards as outlined in the Unified Facilities Criteria (UFC), 4-010-01.

2. All standards were incorporated into the design of the project and have been identified as mandatory items that will not be altered in future design reviews or the construction phase of the project.

3. Additionally, all 13 recommended antiterrorism measures were evaluated and incorporated as outlined in the UFC if applicable.

4. The following standards were included:

Standard 1. Minimum Standoff Distances
Standard 2. Building Separation
Standard 3. Unobstructed Space
Standard 4. Drive-Up/Drop-Off Areas
Standard 5. Access Roads
Standard 6. Parking Beneath Buildings or on Rooftops
Standard 7. Progressive Collapse Avoidance
Standard 8. Structural Isolation
Standard 9. Building Overhangs.
Standard 10. Exterior Masonry Walls
Standard 11. Windows and Glazed Doors
Standard 12. Building Entrance Layout
Standard 13. Exterior Doors
Standard 14. Mailrooms
Standard 15. Roof Access
Standard 16. Overhead Mounted Architectural Features
Standard 17. Air Intakes
Standard 18. Mailroom Ventilation
Standard 19. Emergency Air Distribution Shutoff
Standard 20. Utility Distribution and Installation
Standard 21. Equipment Bracing
Standard 22. Under Building Access
Standard 23. Mass Notification

5. The following recommended additional antiterrorism measures were reviewed and included where applicable to enhance the security of the facility:
(delete the recommendations not included)

Recommendation 1. Vehicle Access Points
Recommendation 2. High-Speed Vehicle Approaches
Recommendation 3. Vantage Points
Recommendation 4. Drive-Up/Drop Off
Recommendation 5. Building Location
Recommendation 6.Railroad Location
Recommendation 7. Access Control for Family Housing
Recommendation 8. Standoff for Family Housing
Recommendation 9. Minimize Secondary Debris
Recommendation 10. Structural Redundancy
Recommendation 11. Internal Circulation
Recommendation 12. Visitor Control
Recommendation 13. Asset Location

6. If you have any additional questions please contact __________ at

________________________________ ____________________________________

Chief Engineer, Project _____ Commander, 20th Civil Engineering
Squadron
20th Civil Engineering Squadron

cc: 20 FW/CCFP

Attachment 14 (Added-SHAWAFB)

PROGRAM ASSISTANCE VISIT OPEN ITEM RESPONSE REPORT

Date

MEMORANDUM FOR 20 FW/CCFP

FROM: (Enter appropriate title)

SUBJECT: Program Assistance Visit (PAV) Finding Response

1. The following is a response to a PAV finding on (enter date of PAV in DD/MM/YY format.)

2. Finding: (Identify the finding. The finding will be outlined in the PAV report generated by 20 FW/CCFP. Retype each finding preceded by its corresponding alphanumeric symbol in parenthesis, just as found in the report. Include the reference, which will also be given in the report.)

3. Corrective Action: (Describe what steps have been taken to correct the finding. Include enough detail in each reply so the AT Office can decide whether to close the finding or keep it open. If your reply action is not complete, describe what you are doing now and include an estimated completion date (ECD). If the finding is beyond the unit's ability to solve, describe the action taken to get help. Please be as specific as necessary, i.e. if the finding requires paperwork, then indicate if the paperwork is completed and who, if anyone, is reviewing/has reviewed it. If the finding requires coordination with outside agencies, then indicate any plans or memorandums that have been completed with that agency.

If no actions have been taken, please indicate so.)

4. ECD: (if applicable)

JOHN E. SMITH, Captain, USAF
20th ___________ Squadron

Attachments:
(Please include copies of any finalized documentation referenced in the "Corrective Action" section